Log Reference for SwitchBlade® x3100 and iMAP Series Switches - Release 15.0 - Issue 1

Acknowledgments

This product includes software developed by the University of California, Berkeley and its contributors.
Copyright ©1982, 1986, 1990, 1991, 1993 The Regents of the University of California. All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).
Copyright ©1998-2008 The OpenSSL Project. All rights reserved.

This product includes software licensed under the GNU General Public License available from:
http://www.gnu.org/licenses/gpl2.html

©2010 Allied Telesis Inc. All rights reserved.

This documentation is subject to change without notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's internal use without the written permission of Allied Telesis, Inc.

Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Additional brands, names and products mentioned herein may be trademarks of their respective companies.

Getting the Most from this Manual

Although you can view this document using Acrobat version 5, to get the best from this manual, we recommend using Adobe Acrobat Reader version 8. You can download Acrobat Reader 8 free from http://www.adobe.com/.

Documentation can be downloaded from the Support area of our website at http://www.alliedtelesis.com. Note that to download software files, you need a valid user account.

Table of Contents

1 Overview of Logs / Alarms System - 1-1

**1 Interfaces for Communicating with Devices - - - - - - - - - - - - - - - - - - -

2.1.11 PSE Device Fault - - -

2.3.2 ARP Filtering Configuration Not Supported - 3-8
2.3.3 ARP Filtering Resources Exceeded - 3-8
2.3.4 Boot Failed - 3-9
2.3.5 Card Diags Failed- 3-10
2.3.6 Config Failed- 3-10
2.3.7 Diags Failed - 3-11
2.3.8 Failed to Access Card - 3-12
2.3.9 Heartbeat Lost - 3-13
2.3.10 Load Card Failed - 3-14
2.3.11 QOS Configuration Failed - 3-15
2.3.12 QOS Configuration Not Supported - 3-16
2.3.13 QOS Resources Exceeded - 3-17
2.3.14 Rate Limiting Failed - 3-18
2.3.15 Reset Failed- 3-18
2.3.16 RTC Battery - 3-19
2.3.17 Simplex - 3-20
2.3.18 Software Version Compatibility - 3-20
2.3.19 Unable to Access Card - 3-21
2.4 CARD023 - atnCardDefectRaised - 3-22
2.4.1 Database in Upgrade Mode - 3-22
2.4.2 File Corruption - 3-23
2.4.3 Inconsistent Load - 3-23
2.4.4 McastGroupLimit- 3-24
2.4.5 Out of Sync- 3-24
2.5 CARD043 - Not Applicable - 3-25
2.5.1 Not Applicable- 3-25
2.6 CFCP001 - atnRedundancyLost - 3-25
2.6.1 Not Applicable- 3-25
2.7 CFCP002 - atnRedundancyRestored - 3-26
2.7.1 Unknown - 3-26
2.8 CFCP014 - atnEpsrNodeTrap - 3-26
2.8.1 Not Applicable- 3-26
2.9 CHAS001 - entConfigChangeTrap - 3-27
2.9.1 Not Applicable- 3-27
2.10 FAN001 - atnFanFaultRaised - 3-27
2.10.1 Fan Module Not Present - 3-27
2.10.2 Fans Not Rotating Properly - 3-27
2.10.3 Hardware Not Recognized - 3-28
2.10.4 High Temperature- 3-28
2.10.5 No Communication- 3-29
2.11 IGMP000 - mcHighWaterMarkPerCardExceeded - 3-29
2.11.1 Not Applicable- 3-29
2.12 IGMP001 - mcChannelLimitPerShelfExceeded - 3-30
2.12.1 Not Applicable- 3-30
2.13 IGMP002 - mcHighWaterMarkPerCardCleared - 3-30
2.13.1 Not Applicable- 3-30
2.14 IGMP003 - mcGroupLimitPerMACExceeded - 3-30
2.14.1 Not Applicable- 3-30

2.15 IGMP004 - mcMACLimitPerPortExceeded ---------- 3-31
2.15.1 Not Applicable ---------- 3-31
2.16 IGMP005 - mcFirstRouterDetected ---------- 3-31
2.16.1 Not Applicable ---------- 3-31
2.17 IGMP006 - mcNewRouterDetected ---------- 3-32
2.17.1 Not Applicable ---------- 3-32
2.18 IGMP007 - mcLastRouterAgedOut ---------- 3-32
2.18.1 Not Applicable ---------- 3-32
2.19 IGMP008 - mcRouterAgedOut ---------- 3-32
2.19.1 Not Applicable ---------- 3-32
2.20 IGMP009 - (no Trap Message) ---------- 3-33
2.20.1 Not Applicable ---------- 3-33
2.21 IGMP010 - (no Trap Message) ---------- 3-33
2.21.1 Not Applicable ---------- 3-33
2.22 INTF003 - (no Trap Message) ---------- 3-34
2.22.1 Classifier Configuration Failed ---------- 3-34
2.22.2 Classifier Configuration Not Supported ---------- 3-34
2.22.3 Classifier Resources Exceeded ---------- 3-35
2.23 IPIF001 - (To Be Supplied) ---------- 3-35
2.23.1 IP Interface Configuration Failed ---------- 3-35
2.24 LOG005 - atnMediaLogStreamError ---------- 3-36
2.24.1 I/O error writing to compact flash ---------- 3-36
2.24.2 Compact flash unit deactivated ---------- 3-36
2.24.3 Compact flash media not present ---------- 3-36
2.25 LOG006 - Not Applicable ---------- 3-37
2.25.1 Not Applicable ---------- 3-37
2.26 PORT003 - Linkdown ---------- 3-37
2.26.1 BFD Detected Miswiring ---------- 3-37
2.26.2 BFD Session Failed ---------- 3-38
2.26.3 Config Failed ---------- 3-38
2.26.4 Disable Failed ---------- 3-39
2.26.5 Enable Failed ---------- 3-40
2.26.6 Loss of Frame (LOF) ---------- 3-40
2.26.7 Loss of Link (LOL) ---------- 3-41
2.26.8 Loss of Signal (LOS) ---------- 3-41
2.26.9 Loss of Sync (LOSY) ---------- 3-42
2.26.10 Remote BFD Session Failed ---------- 3-42
2.26.11 Reset Failed ---------- 3-43
2.26.12 SFP Not Present ---------- 3-43
2.26.13 Unexpected BPDU Received ---------- 3-43
2.26.14 XFP Not Present ---------- 3-44
2.27 PORT005 - atnPortDefectRaised ---------- 3-44
2.27.1 Classifier Configuration Failed ---------- 3-44
2.27.2 Classifier Configuration Not Supported ---------- 3-45
2.27.3 Classifier Resources Exceeded ---------- 3-46
2.28 RMON001 - risingAlarm ---------- 3-46
2.28.1 Not Applicable ---------- 3-46

2.29 RMON002 - fallingAlarm ---------- 3-47
2.29.1 Not Applicable---------- 3-47
2.30 SHLF001 - atnShelfFaultRaised ---------- 3-47
2.30.1 Port Outage Threshold---------- 3-47
2.30.2 VLAN has no NETWORK facing interface ---------- 3-48
2.31 SYS004 - atnCardDefectRaised---------- 3-48
2.31.1 Database Audit Failure ---------- 3-48
2.31.2 Database Transaction Failure ---------- 3-49
2.31.3 Death of non-critical task---------- 3-50
2.31.4 Flash Write Failure---------- 3-50
2.32 SYS009 - atnShelfFaultRaised ---------- 3-51
2.32.1 Cannot Read MAC Address---------- 3-51
2.33 TRAP003 - coldStartTrap---------- 3-51
2.33.1 Not Applicable---------- 3-51
2.34 TRAP004 - warmStart ---------- 3-52
2.34.1 Not Applicable---------- 3-52
2.35 TRAP009 - entConfigChangeTrap---------- 3-52
2.35.1 Not Applicable---------- 3-52

4 iMAP Logs with Traps ----------4-1

1 Overview ---------- 4-1
1.1 Listing of Logs and Traps---------- 4-1
1.2 Log and Trap Listing by Reason Code ---------- 4-1

2 Listing of Logs and Traps ---------- 4-2
2.1 ADSL021- adslAtucPerfLofsThreshTrap ---------- 4-9
2.1.1 Not Applicable---------- 4-9
2.2 ADSL022 - adslAturPerfLossThreshTrap---------- 4-10
2.2.1 Not Applicable---------- 4-10
2.3 ADSL024 - adslAtucPerfLprsThreshTrap---------- 4-10
2.3.1 Not Applicable---------- 4-10
2.4 ADSL025 - adslAtucPerfESsThreshTrap ---------- 4-11
2.4.1 Not Applicable---------- 4-11
2.5 ADSL026 - adslAturPerfLofsThreshTrap---------- 4-11
2.5.1 Not Applicable---------- 4-11
2.6 ADSL028 - adslAturPerfLprsThreshTrap---------- 4-12
2.6.1 Not Applicable---------- 4-12
2.7 ADSL029 - adslAturPerfESsThreshTrap ---------- 4-12
2.7.1 Not Applicable---------- 4-12
2.8 ADSL030 - adslAtucPerfSesLThreshTrap ---------- 4-13
2.8.1 Not Applicable---------- 4-13
2.9 ADSL031 - adslAtucPerfUasLThreshTrap ---------- 4-13
2.9.1 To Be Supplied ---------- 4-13
2.10 ADSL032 - adslAturPerfSesLThreshTrap---------- 4-14
2.10.1 Not Applicable---------- 4-14

2.11 ADSL033 - adslAturPerfUasLThreshTrap ---- 4-14
2.11.1 Not Applicable ---- 4-14
2.12 ADSL034 - adslAtucFailedFastRThreshTrap ---- 4-15
2.12.1 Not Applicable ---- 4-15
2.13 CARD001 - entConfigChangeTrap ---- 4-15
2.13.1 Slot Provisioning Mismatch ---- 4-15
2.14 CARD005 - atnCardDefectRaised ---- 4-16
2.14.1 DSP Core Fault ---- 4-16
2.14.2 Power 18 Failed ---- 4-17
2.14.3 Power 25 Adj. Failed ---- 4-17
2.14.4 Power A Failed ---- 4-18
2.14.5 Power B Failed ---- 4-18
2.14.6 Power Fuse Failed ---- 4-19
2.14.7 SB 2.5v Power Failed ---- 4-19
2.14.8 SB CPU 2.5v Power Failed ---- 4-20
2.14.9 SB 2.5v ANALOG Power Failed ---- 4-20
2.14.10 SB 2.5v DIGITAL Power Failed ---- 4-21
2.14.11 Ring Generator Overload ---- 4-21
2.14.12 Ring Generator Failure ---- 4-21
2.14.13 Lost Communication with Call Server ---- 4-22
2.14.14 DSP Failure ---- 4-22
2.14.15 Configuration Incomplete ---- 4-22
2.14.16 Hardware Unsupported ---- 4-23
2.14.17 Incompatible with Active ---- 4-23
2.14.18 Internal Oscillator Failure ---- 4-24
2.14.19 Unable to Load ---- 4-24
2.14.20 DNS Server Timed Out ---- 4-24
2.14.21 ARP Resolution Failed ---- 4-25
2.14.22 DNS resolution failed ---- 4-25
2.14.23 CFlash Failed ---- 4-25
2.14.24 AC Power A Failed ---- 4-26
2.14.25 AC Power B Failed ---- 4-26
2.14.26 AC Power A Fan Failed ---- 4-27
2.14.27 AC Power B Fan Failed ---- 4-27
2.14.28 1.2v Power Failed ---- 4-27
2.14.29 Duplicate IP Address ---- 4-28
2.14.30 IP buffer pool exhausted ---- 4-28
2.14.31 Power Input Incompatibility ---- 4-29
2.14.32 Inconsistent Flooding ---- 4-30
2.14.33 Card Disable Failed ---- 4-30
2.14.34 Protocol Mismatch ---- 4-31
2.14.35 Incompatible Load ---- 4-31
2.14.36 Unsupported Hardware ---- 4-32
2.15 CARD023 - atnCardDefectRaised ---- 4-32
2.15.1 Sync Card Not Detected ---- 4-32
2.15.2 Loss of Primary Reference ---- 4-32
2.15.3 Loss of Secondary Reference ---- 4-33
2.15.4 Loss of Holdover ---- 4-33

2.15.5 Sync Card Clock Error ---------- 4-34
2.16 CARD046 - ATNCARDFDBMGMTOVERFLOW ---------- 4-34
2.16.1 Not Applicable ---------- 4-34
2.17 CUC001 - atnCUCFaultRaised ---------- 4-35
2.17.1 Not Present ---------- 4-35
2.17.2 Power Supply Failure ---------- 4-35
2.17.3 No Communication ---------- 4-35
2.18 FAN001 - atnCUCFaultRaised ---------- 4-36
2.18.1 Hardware Not Recognized ---------- 4-36
2.19 FAN001 - atnFanFaultRaised ---------- 4-36
2.19.1 Fan Module Power Supply Failure ---------- 4-36
2.20 INTF001 - Linkdown ---------- 4-36
2.20.1 All parents non-administratively down ---------- 4-36
2.20.2 Config Failed ---------- 4-37
2.20.3 Echo Request Timeout ---------- 4-37
2.20.4 Loopback Detected ---------- 4-38
2.20.5 Negotiation Failed ---------- 4-38
2.20.6 Peer Disabled ---------- 4-39
2.20.7 ONU Not Discovered ---------- 4-39
2.20.8 Remote Tranmsit Failed ---------- 4-39
2.20.9 Loading Firmware ---------- 4-40
2.20.10 Waiting to Load Firmware ---------- 4-40
2.20.11 Not Applicable ---------- 4-41
2.20.12 All Links Failed ---------- 4-41
2.20.13 Unexpected BPDU Received ---------- 4-41
2.20.14 Report Timeout ---------- 4-42
2.20.15 Links Not Discovered ---------- 4-42
2.20.16 All ASM Links Down ---------- 4-43
2.20.17 All Parent Interfaces Down ---------- 4-43
2.20.18 Loss of Signal (LOS) ---------- 4-43
2.20.19 Alarm Indication Signal ---------- 4-44
2.20.20 SFP Type Mismatch ---------- 4-44
2.20.21 SFP Not Present ---------- 4-44
2.20.22 Receive Loss of Lock ---------- 4-45
2.20.23 Remote Defect Indication ---------- 4-45
2.21 INTF003 - Unknown ---------- 4-45
2.21.1 Bandwidth Degraded ---------- 4-45
2.22 INTF003 - atnInterfaceDefectRaised ---------- 4-46
2.22.1 Keep Alive Timeout ---------- 4-46
2.22.2 Remote Loss of Signal (UNI) ---------- 4-47
2.22.3 Remote Gate Timeout ---------- 4-47
2.22.4 Remote Keep Alive Timeout ---------- 4-47
2.22.5 Mismatched ONU Type ---------- 4-48
2.22.6 Unsupported ONU Type ---------- 4-48
2.22.7 No Response from BRAS ---------- 4-49
2.22.8 Negotiation Failed ---------- 4-49
2.22.9 Echo Request Timeout ---------- 4-49
2.22.10 Below Min Downstream Aggregate Rate ---------- 4-50

2.22.11 Below Min Upstream Aggregate Rate - 4-50
2.22.12 Downstream Differential Rate Exceeded - 4-51
2.22.13 Some ASM Links Down - 4-51
2.22.14 Some Parent Interfaces Down - 4-51
2.22.15 Status Attribute - 4-52
2.22.16 Upstream Differential Rate Exceeded - 4-52
2.22.17 Excessive Zeroes - 4-52
2.22.18 Bipolar Violation - 4-53
2.22.19 Far-End SEF AIS - 4-53
2.22.20 Out of Frame - 4-53
2.23 INTF003 - Linkdown - 4-54
2.23.1 Loss of Frame (LOF) - 4-54
2.24 PMON001 - atnDs1CurrentLCVThreshTrap - 4-54
2.24.1 Not Applicable - 4-54
2.25 PMON002 - atnDs1CurrentLESThreshTrap - 4-54
2.25.1 Not Applicable - 4-54
2.26 PMON003 - atnDs1CurrentLOSThreshTrap - 4-55
2.26.1 Not Applicable - 4-55
2.27 PMON004 - atnDs1CurrentSESThreshTrap - 4-55
2.27.1 Not Applicable - 4-55
2.28 PMON005 - atnDs1DayUASThreshTrap - 4-56
2.28.1 Not Applicable - 4-56
2.29 PORT003 - Linkdown - 4-56
2.29.1 CAS Thermal Shutdown - 4-56
2.29.2 SLIC Thermal Shutdown - 4-56
2.29.3 AC Fault - 4-57
2.29.4 DC Fault - 4-57
2.29.5 PCM Clock Failure - 4-57
2.29.6 Battery Failure - 4-58
2.29.7 No Peer Present (NPP) - 4-58
2.29.8 Loopback Failed - 4-58
2.29.9 Timing Reference Failed - 4-59
2.29.10 Link Quality Failed - 4-59
2.29.11 Loss of RTP Receive Stream - 4-60
2.29.12 Loss of RTP Transmit Stream - 4-60
2.29.13 Receiving AIS - 4-60
2.29.14 Receiving RAI - 4-61
2.29.15 Transmit Failed - 4-61
2.29.16 No Links Discovered - 4-62
2.29.17 Loading Firmware - 4-62
2.29.18 Interface Internal Failure - 4-62
2.29.19 Registration Failed - 4-63
2.29.20 DS3 Out of Service - 4-63
2.30 PORT005 - HDSL2SHDSLPERFLOSWSTHRESH - 4-63
2.30.1 Loss Of Sync Word - 4-63
2.31 PORT005 - atnPortDefectRaised - 4-64
2.31.1 Loss Of Signal Quality (LOSQE) - 4-64
2.31.2 Loss of Power - Modem Off (LPR) - 4-64

2.31.3 Transmit Degraded - - -

2.47 XDSL004 - HDSL2SHDSLPERFSESTHRESH ---- 4-78
2.47.1 Not Applicable ---- 4-78
2.48 XDSL005 - HDSL2SHDSLPERFUASTHRESH ---- 4-78
2.48.1 Not Applicable ---- 4-78
2.49 XDSL006 - HDSL2SHDSLPERFLOSWSTHRESH ---- 4-79
2.49.1 Not Applicable ---- 4-79
2.50 XDSL007 - HDSL2SHDSLPERFCRCANOMALIESTHRESH ---- 4-79
2.50.1 Not Applicable ---- 4-79
2.50.2 Not Applicable ---- 4-79
2.51 XDSL008 - HDSL2SHDSLPERFESTHRESH ---- 4-80
2.51.1 Not Applicable ---- 4-80
2.52 XDSL009 - HDSL2SHDSLPERFSESTHRESH ---- 4-80
2.52.1 Not Applicable ---- 4-80
2.53 XDSL010 - HDSL2SHDSLPERFUASTHRESH ---- 4-81
2.53.1 Not Applicable ---- 4-81
2.54 XDSL018 - xdslPortQualityRetrain ---- 4-81
2.54.1 Retrain: Line Quality ---- 4-81
2.55 XDSL019 - xdslPortStuckHandShakeRetrain ---- 4-81
2.55.1 Retrain: Handshake Stuck ---- 4-81
2.56 XDSL020 - xdslPortMinDownRateRetrain ---- 4-82
2.56.1 Retrain: Minimum Downstream Rate ---- 4-82
2.57 XDSL021 - xdsllossofmarginretrain ---- 4-82
2.57.1 Retrain: SNR Margin Threshold ---- 4-82

5 NMS Logs ---- 5-1

1 Overview ---- 5-1

2 Device Backup ---- 5-1
2.1 Device Backup Failed ---- 5-1

3 Discovery ---- 5-2
3.1 SNMP Error Code ---- 5-2
3.2 Unable to Detect MO ---- 5-2
3.3 Max. Allowed Node Limit Reached ---- 5-2
3.4 Unable to login to device ---- 5-2
3.5 Detected DUPLICATE IP ---- 5-2

4 NMS backup ---- 5-3
4.1 Cannot locate directory ---- 5-3
4.2 Cannot create directory ---- 5-3
4.3 IO Exception to access NMS Home directory ---- 5-3
4.4 IO Exception to access backup directory ---- 5-3
4.5 Cannot locate directory ---- 5-3
4.6 Security Exception ---- 5-3
4.7 Cannot complete backup ---- 5-4

4.8 Cannot create directory for directory copy ---------- 5-4

5 Status Poll ---------- 5-4

5.1 At least one Node in failure state ---------- 5-4

5.2 Interface Failure ---------- 5-4

5.3 Node Failure ---------- 5-4

6 Other ---------- 5-5

6.1 Upload Config Failed ---------- 5-5

1. Overview of Logs / Alarms System

1 Interfaces for Communicating with Devices

To receive event and alarm indicators from the Allied Telesis devices, interfaces must have been configured so that these indicators are sent to the proper place and are filtered when necessary. This Section provides an overview of these interfaces.

Note: It is assumed that the user has set up the interfaces described in this Section and can readily communicate with the system through the MGMT or inband upstream port. However, a condition or conditions may exist where the user cannot communicate with the system or the user is not receiving logs on their configured log server or the NMS. If the condition(s) cannot be cleared, the user should contact Allied Telesis Technical Support.

1.1 The Command Line Interface (CLI)

One of two IP interfaces can be used that allow the Allied Telesis product to communicate with management systems.

- The MGMT Ethernet interface that transports only management data packets.
- An in-band Ethernet interface that interleaves user data packets with management data packets on the uplink, using a VLAN interface. In using a VLAN interface the management data packets are always VLAN-tagged.

Over these two interfaces, the TELNET or SNMP agent can be configured.

Note: Only one interface can be enabled at a time; enabling an interface will disable an interface already enabled. If necessary, the ENABLE IP INTERFACE command will automatically disable the other IP Interface.

Note: These interfaces should be set up using the local RS232 interface. See the following Caution

Caution: ***If the user disables or deletes an IP interface, and the user is currently using that interface to communicate with the Allied Telesis product, the interface will be immediately disconnected.***

1.1.1 PING

The system provides the user with the ability to ***ping*** network devices from the CLI command line interface.

An example of the PING command:

officer SEC> PING 172.16.17.18

officer SEC> PING 172.16.17.18 (172.16.17.18)

64 bytes from 172.16.17.18 (172.16.17.18): icmp_seq=1

--- 172.16.17.18 ping statistics ---

1 packets transmitted, 1 packets received, 0% packet loss

TABLE 1-1 PING command

Noun	Verb	Syntax	Description

PING	PING	PING={ ipaddress
		  | hostname
		  }
		[FROM
		  { INTERFACE={ type:id
		  | id
		  | ifname
		  }
		  | IPADDRESS=ipaddress
		  }]
		[DELAY=1..900]
		[LENGTH=1..8192]
		[NUMBER={ 1..65535
		  | CONTINUOUS
		  }]
		[TIMEOUT=1..900]
			The PING command provides the user with the ability to determine whether a network device is accessible or not.

1.2 The AlliedView Network Management System (NMS)

Just as the Allied Telesis devices can be set up to report certain events over certain interfaces, the AlliedView NMS product uses parsing and filtering to ensure that any change of state in a device or set of devices can be accessed and highlighted immediately.

To report events and alarms, the Allied AlliedView NMS uses the following tools:

Note: For a complete description of the AlliedView NMS parsing and filtering tools, refer to the *AlliedView NMS Administration Guide*.

- Trap Parser

  The Trap Parser creates and refines the information received from traps (specific unsolicited reports by a device). These have the standard SNMP fields (sysOID, access agent, text strings, etc.).

Note: Trap parsers are critical to alarm correlation and should only be changed under the supervision of Allied Telesis Technical Support personnel. Refer to Section 3 for a listing of traps produced by Allied Telesis devices.

- Event Parser

The traps are then forwarded to the Event Parser, where administrators can change and add various attributes of the trap such as severity or the text message, as well as provide further parsers. Also sent to the Event Parser are information only events about the activity of the AlliedView NMS.

Note: As with the Trap Parser, administrators should consult with Allied Telesis personnel before changing attributes, such as severity, since this determines what will appear as alarms.

- Event Filter

  Event Filters provides a way to setting a matching criteria to filter events and then configuring an action (such as an email) for these events.

- Alarm Screen

  The events that have a severity are considered alarms and are displayed on the alarm screen. To access the alarm view, select the node **Alarms** from the NMS Tree to view the Alarms, as shown in the following figure The alarm screen is a table that lists all of the events that have a severity (or are Clear). The alarms can be sorted by clicking on the column. Refer to the *AlliedView NMS User Guide* for details on navigating and refining the view, as well as using the Search tool.

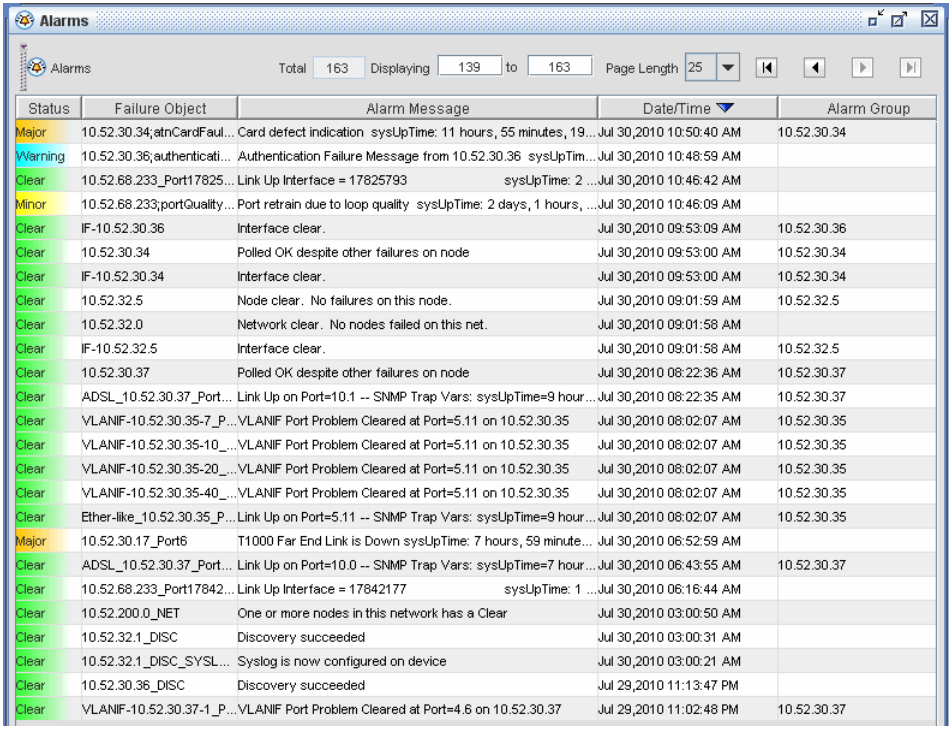
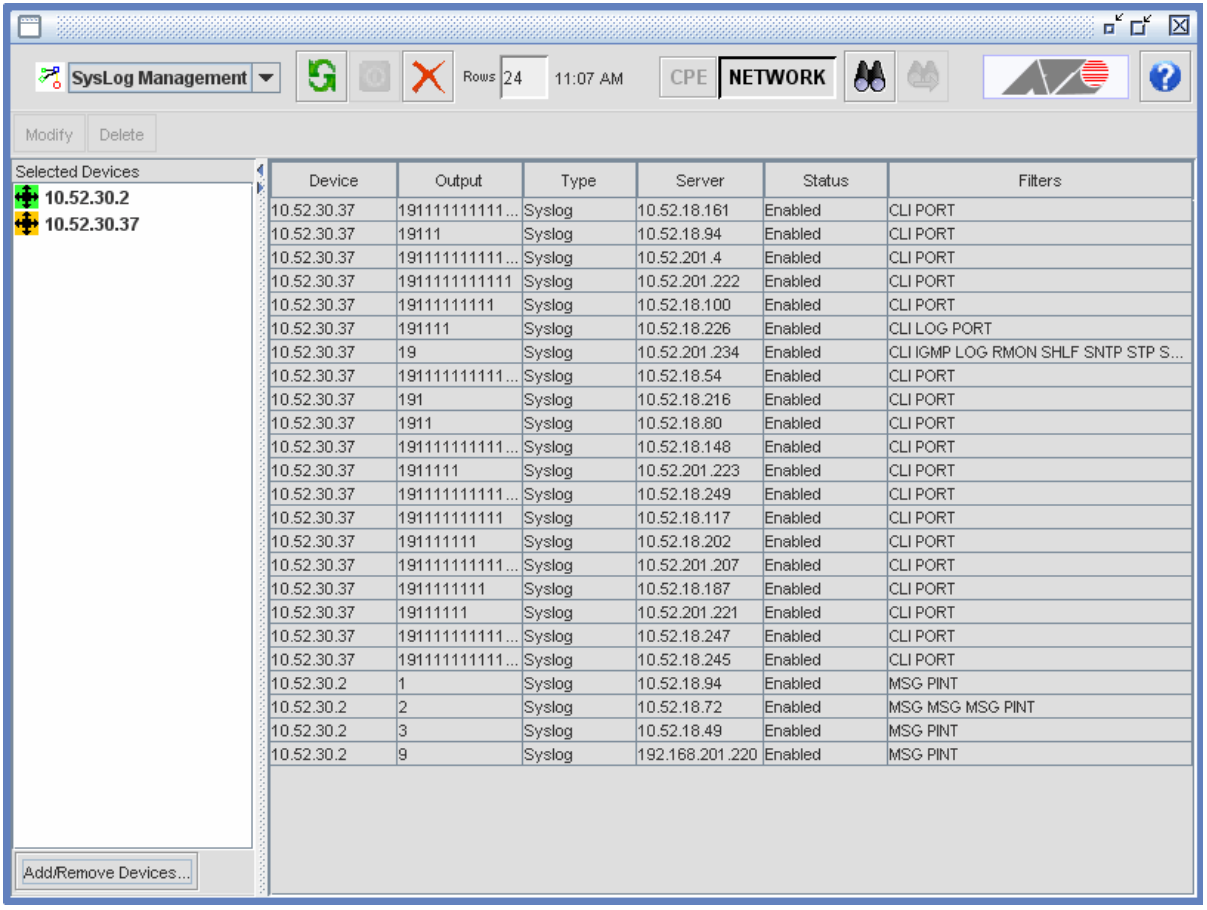

Alarms
Alarms
Total 163 Displaying 139 to 163 Page Length 25
Status | Failure Object | Alarm Message | Date/Time | Alarm Group
Major | 10.52.30.34;atnCardFaul... | Card defect indication sysUpTime: 11 hours, 55 minutes, 19... | Jul 30,2010 10:50:40 AM | 10.52.30.34
Warning | 10.52.30.36;authenticati... | Authentication Failure Message from 10.52.30.36 sysUpTim... | Jul 30,2010 10:48:59 AM |
Clear | 10.52.68.233_Port17825... | Link Up Interface = 17825793 sysUpTime: 2 ... | Jul 30,2010 10:46:42 AM |
Minor | 10.52.68.233;portQuality... | Port retrain due to loop quality sysUpTime: 2 days, 1 hours, ... | Jul 30,2010 10:46:09 AM |
Clear | IF-10.52.30.36 | Interface clear. | Jul 30,2010 09:53:09 AM | 10.52.30.36
Clear | 10.52.30.34 | Polled OK despite other failures on node | Jul 30,2010 09:53:00 AM | 10.52.30.34
Clear | IF-10.52.30.34 | Interface clear. | Jul 30,2010 09:53:00 AM | 10.52.30.34
Clear | 10.52.32.5 | Node clear. No failures on this node. | Jul 30,2010 09:01:59 AM | 10.52.32.5
Clear | 10.52.32.0 | Network clear. No nodes failed on this net. | Jul 30,2010 09:01:58 AM |
Clear | IF-10.52.32.5 | Interface clear. | Jul 30,2010 09:01:58 AM | 10.52.32.5
Clear | 10.52.30.37 | Polled OK despite other failures on node | Jul 30,2010 08:22:36 AM | 10.52.30.37
Clear | ADSL_10.52.30.37_Port... | Link Up on Port=10.1 -- SNMP Trap Vars: sysUpTime=9 hour... | Jul 30,2010 08:22:35 AM | 10.52.30.37
Clear | VLANIF-10.52.30.35-7_P... | VLANIF Port Problem Cleared at Port=5.11 on 10.52.30.35 | Jul 30,2010 08:02:07 AM | 10.52.30.35
Clear | VLANIF-10.52.30.35-10_... | VLANIF Port Problem Cleared at Port=5.11 on 10.52.30.35 | Jul 30,2010 08:02:07 AM | 10.52.30.35
Clear | VLANIF-10.52.30.35-20_... | VLANIF Port Problem Cleared at Port=5.11 on 10.52.30.35 | Jul 30,2010 08:02:07 AM | 10.52.30.35
Clear | VLANIF-10.52.30.35-40_... | VLANIF Port Problem Cleared at Port=5.11 on 10.52.30.35 | Jul 30,2010 08:02:07 AM | 10.52.30.35
Clear | Ether-like_10.52.30.35_P... | Link Up on Port=5.11 -- SNMP Trap Vars: sysUpTime=9 hour... | Jul 30,2010 08:02:07 AM | 10.52.30.35
Major | 10.52.30.17_Port6 | T1000 Far End Link is Down sysUpTime: 7 hours, 59 minute... | Jul 30,2010 06:52:59 AM |
Clear | ADSL_10.52.30.37_Port... | Link Up on Port=10.0 -- SNMP Trap Vars: sysUpTime=7 hour... | Jul 30,2010 06:43:55 AM | 10.52.30.37
Clear | 10.52.68.233_Port17842... | Link Up Interface = 17842177 sysUpTime: 1 ... | Jul 30,2010 06:16:44 AM |
Clear | 10.52.200.0_NET | One or more nodes in this network has a Clear | Jul 30,2010 03:00:50 AM |
Clear | 10.52.32.1_DISC | Discovery succeeded | Jul 30,2010 03:00:31 AM |
Clear | 10.52.32.1_DISC_SYSL... | Syslog is now configured on device | Jul 30,2010 03:00:21 AM |
Clear | 10.52.30.36_DISC | Discovery succeeded | Jul 29,2010 11:13:47 PM |
Clear | VLANIF-10.52.30.37-1_P... | VLANIF Port Problem Cleared at Port=4.6 on 10.52.30.37 | Jul 29,2010 11:02:48 PM | 10.52.30.37

FIGURE 1-1 Alarm View Main Panel

- System Logs

  System logs are stored in the NMS database as they are received. The actual logs stored depend on the log types that are enabled and the log filters applied to each managed device. You can view all of the logs received on your network from the System Log Events subview of the Network Events view. You can also view logs on a specific device by right-clicking the device and then selecting ***Provision -> Device Log Viewer*** from the pop-up menu. The Log Management Viewer window, shown in the following figure, will appear. Refer to the *AlliedView NMS User Guide* for detailed information on the System Log Events subview.



Device	Output	Type	Server	Status	Filters
10.52.30.37	191111111111...	Syslog	10.52.18.161	Enabled	CLI PORT
10.52.30.37	19111	Syslog	10.52.18.94	Enabled	CLI PORT
10.52.30.37	191111111111...	Syslog	10.52.201.4	Enabled	CLI PORT
10.52.30.37	1911111111111	Syslog	10.52.201.222	Enabled	CLI PORT
10.52.30.37	19111111111	Syslog	10.52.18.100	Enabled	CLI PORT
10.52.30.37	191111	Syslog	10.52.18.226	Enabled	CLI LOG PORT
10.52.30.37	19	Syslog	10.52.201.234	Enabled	CLI IGMP LOG RMON SHLF SNTP STP S...
10.52.30.37	191111111111...	Syslog	10.52.18.54	Enabled	CLI PORT
10.52.30.37	191	Syslog	10.52.18.216	Enabled	CLI PORT
10.52.30.37	1911	Syslog	10.52.18.80	Enabled	CLI PORT
10.52.30.37	191111111111...	Syslog	10.52.18.148	Enabled	CLI PORT
10.52.30.37	1911111	Syslog	10.52.201.223	Enabled	CLI PORT
10.52.30.37	191111111111...	Syslog	10.52.18.249	Enabled	CLI PORT
10.52.30.37	191111111111	Syslog	10.52.18.117	Enabled	CLI PORT
10.52.30.37	191111111	Syslog	10.52.18.202	Enabled	CLI PORT
10.52.30.37	191111111111...	Syslog	10.52.201.207	Enabled	CLI PORT
10.52.30.37	1911111111	Syslog	10.52.18.187	Enabled	CLI PORT
10.52.30.37	19111111	Syslog	10.52.201.221	Enabled	CLI PORT
10.52.30.37	191111111111...	Syslog	10.52.18.247	Enabled	CLI PORT
10.52.30.37	191111111111...	Syslog	10.52.18.245	Enabled	CLI PORT
10.52.30.2	1	Syslog	10.52.18.94	Enabled	MSG PINT
10.52.30.2	2	Syslog	10.52.18.72	Enabled	MSG MSG MSG PINT
10.52.30.2	3	Syslog	10.52.18.49	Enabled	MSG PINT
10.52.30.2	9	Syslog	192.168.201.220	Enabled	MSG PINT

FIGURE 1-2 Log Management Viewer

1.3 AlliedView NMS Messages for the NMS Configuration

There is a set of messages that the NMS produces when there is a problem with the NMS itself. These can be divided into the following areas:

- Status Polling of Devices
- Discovery of Devices
- NMS Backup
- Device Backup

These messages are included in Section 4 and are listed as messages with the Category NMS.

2 Types of Alarm Indicators

When the OAM system is configured as described in Chapter 3 of the **iMAP User Guide**, indicators for faults or potential faults are easy to generate, store, and output. The OAM system produces the following event and alarm indications: logs, Traps, and LED alarm indicators. These events are described in more detail below.

2.1 Alarm Severity

Allied Telesis system alarms are organized by order of severity level. They are Critical, Major, and Minor. Each level is described here.

2.1.1 Critical

Critical is the highest, most severe level of alarm. An alarm with a severity level of critical means that system service is being detrimentally affected. It requires the user's immediate attention.

When a critical alarm conditions is raised, the CRIT LED on the CFC faceplate will be illuminated. An LED on a card faceplate may also be illuminated.

A log indicating a critical alarm will be prefaced by "***C**" as the first two characters in the first line of text. An example of a critical alarm log is shown below.

```
*C SYS009 2003-12-04 13:29:57 0327 FAULT
System: Raised Port Outage Threshold
```

2.1.2 Major

Major is the second highest level of alarm. An alarm with a severity level of major means that system service may be affected. The user must immediately investigate a major alarm.

When a major alarm conditions is raised, the MAJOR LED on the CFC faceplate will be illuminated. An LED on a card faceplate may also be illuminated.

A log indicating a major alarm will be prefaced by "******" as the first two characters in the first line of text. An example of a major alarm log is illustrated below.

```
** PORT003 2003-12-04 13:30:04 0356 FAULT
```

```
Location: Slot: 5 Port: 1
Description: Port Fault Set
Reason Code: Loss Of Link
```

2.1.3 Minor

Minor is the lowest level of alarm. An alarm with a severity level of minor means that system service is not affected. However, this alarm condition could lead to a major or critical alarm condition; therefore, the user should investigate the alarm.

When a minor alarm conditions is raised, the MINOR LED on the CFC faceplate will be illuminated. An LED on a card faceplate may also be illuminated.

A log indicating a minor alarm will be prefaced by "*" as the first character in the first line of text. An example of a minor alarm log is illustrated below.

```
 * SYS009 2003-12-04 15:20:31 2669 FAULT
System: Raised Port Outage Threshold
```

Some alarm conditions begin as a minor alarm, but as the alarm condition continues, its level will be raised. For example, a port outage threshold alarm may initially be raised as a minor alarm. However, if more ports encounter the same alarm condition and the number of ports in alarm increases, after a certain threshold is reached, the alarm will become a major alarm. Furthermore, if the alarm condition continues and even more ports encounter the same alarm condition and the number of ports in alarm increases, after a third threshold is reached, the alarm will become a critical alarm. Thresholds for this example, a port outage, are:

- Minor - Less than 24 downstream ports are impacted by card failures and there is at least one uplink available.
- Major - More than 24 but less than 128 downstream links are impacted by card faults and there is at least one uplink available.
- CRITICAL - More than 128 downstream ports are impacted by card faults and/or there is no uplink available.

2.2 Port Outage Threshold Configuration

Port outage thresholds can be configured to be either MAJOR, MINOR, or CRITIAL.

An example follows:

```
SHOW ALARMS THRESHOLD
 Threshold Mark
 -------------------------------------
 MINOR                                1
 MAJOR                                24
 CRITICAL                             128

SET ALARMS THRESHOLD MINOR=7 MAJOR=32 CRITICAL=96
Warning(033613): 6 ports can go out of service before
an alarm is raised if the MINOR threshold is 7.
 Threshold Mark
 -------------------------------------
 MINOR                                7
```

```
 MAJOR                                32
 CRITICAL                             96
 Info (010017): Operation Successful

SETDEFAULTS ALARMS THRESHOLD
 Threshold Mark
 -------------------------------------
 MINOR                                1
 MAJOR                                24
 CRITICAL                             128
 Info (010017): Operation Successful

officer SEC>> SHOW ALARMS THRESHOLD
 Threshold Mark
 -------------------------------------
 MINOR                                1
 MAJOR                                24
 CRITICAL                             128
```

Note that the system will default to known thresholds if they have not been configured. Defaults are:

MINOR - Less than or 24 ports

MAJOR - 25-127 ports

CRITICAL - More than 128 port

TABLE 1-2 Port Outage Thresholds commands

Noun	Verb	Syntax	Description
ALARMS THRESHOLD	SET	SET ALARMS THRESHOLD [MINOR=value] [MAJOR=value] [CRITICAL=value]	The alarm thresholds control when the MINOR, MAJOR, and CRITICAL Port Outage Threshold alarms are raised. The values must be non-zero and satisfy the condition of MINOR, MAJOR, or CRITICAL. These signify the lowest number of ports for that alarm to be raised. Critical - Minimum number of ports before a CRITICAL alarm is raised. Major - Minimum number of ports before a MAJOR alarm is raised. Minor - Minimum number of ports before a MINOR alarm is raised. Setting minor to anything greater than one is allowed, but not recommended.That means that (MINOR - 1) ports can be out of service before the threshold alarm is raised. Note: When all UPLINK ports are out of service, a CRITICAL alarm will be raised regardless of the threshold values.
ALARMS THRESHOLD	SETDEFAULTS	SETDEFAULTS ALARMS THRESHOLD	This command sets all alarm threshold values back to the factory defaults.
ALARMS THRESHOLD	SHOW	SHOW ALARMS THRESHOLD	Displays the current settings for port alarm thresholds.

2.3 Logs

Allied Telesis products provide totally flexible logging functionality.

Note that logs are the way to find out about troubles since all events produce logs and all logs with traps are sent to NMS, where the interface can be customized, as explained in 1.2.

2.4 Traps

Refer to the *SBx3112 Software Reference Manual* for details about the SNMP parameter SNMPTRAPFILTER and instructions for configuring SNMP and monitoring for traps. The user can customize the output of traps. For example, users can determine where trap output will be sent, select the severity and category of the reported traps, etc.

2.5 Relationship of Logs and Traps with Device Interfaces

Since there are multiple ways to report a device status as well as multiple interfaces to display them, the following summarizes how they are related:

Traps are produced and associated with:

- Standard (RFC-based) MIBs
- Allied Telesis products

All traps produce logs, and these logs have associated log messages, reason codes, and severities.

Some logs, on the other hand, do not have an associated trap. These are usually for status or update information.

The SYSLOG (System Log Events) application on the AlliedView NMS shows the logs as produced by the Allied Telesis devices and can be controlled to show only some or all log categories. The Syslog viewer, therefore, is a way to view **all** logs produced by the devices on the AlliedView NMS, while the Alarm view is a graphical way to view all log messages that have a severity and need to be viewed immediately.

2.6 CARD and PORT Logs (Information, Degrading and Failing Conditions)

The two most common logs for card and port logs are CARD023, CARD005, PORT013, and PORT003 logs.

- CARD023 logs are intended to indicate INFO conditions that do not affect state, such as file corruption, database upgrade, multicast stream limit, and inconsistent load.
- CARD005 covers all failing and degrading conditions.

Note: Both of those logs generate the same SNMP trap.

- PORT003 logs are for degrading conditions, and PORT013 is informational only.

3 Log Formats

The Allied Telesis product produces management logs that provide information about all changes that occur. Figure 1-3 shows an example log.

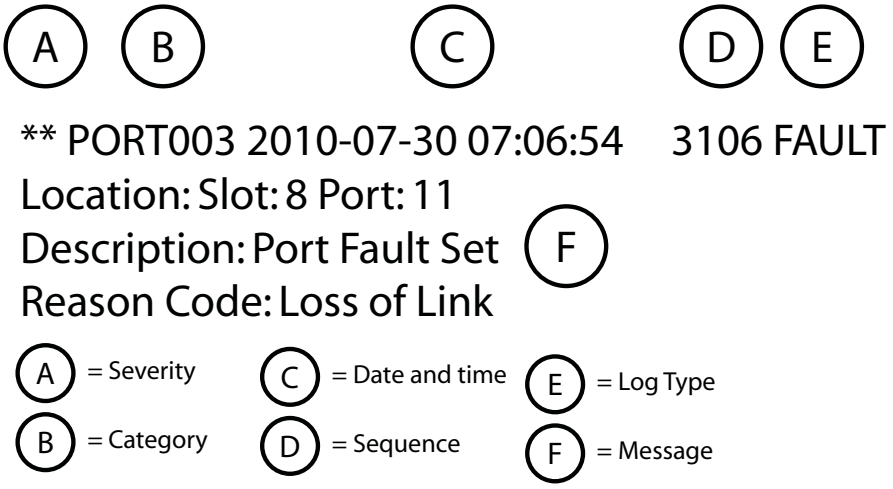


FIGURE 1-3 Sample Log Produced by the Allied Telesis Product (SBx3112)

3.1 Log Messages from the CLI

Use the SHOW LOG command to filter logs immediately in the output, for example to show only logs that have a severity of CRITICAL.

3.2 Examples

Examples of system logs follow:

3.2.1 Informational (INFO) logs

These logs record events that may have an associated trap.

Note: Logs that have an associated trap are the main focus of this document.

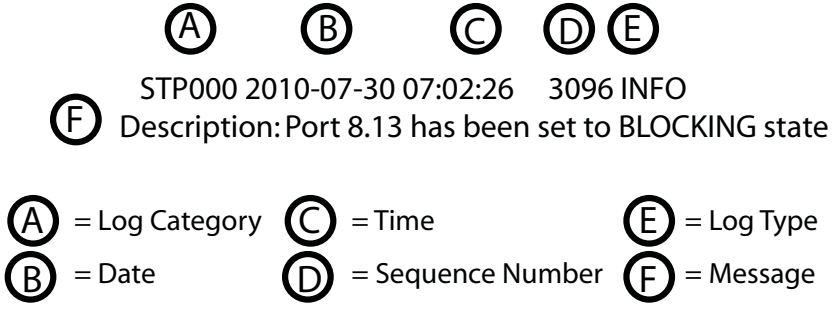


FIGURE 1-4 Informational log

3.2.2 Fault logs

These are the logs that have associated traps as well as reason codes and are the ones included in this document. Refer to Figure 1-3.

3.2.3 Other logs

Logs of the type OTHER are for events such as a change of state and are useful for monitoring system activity as the system goes through changes in configuration. Some logs can have associated traps and these are included in this document.

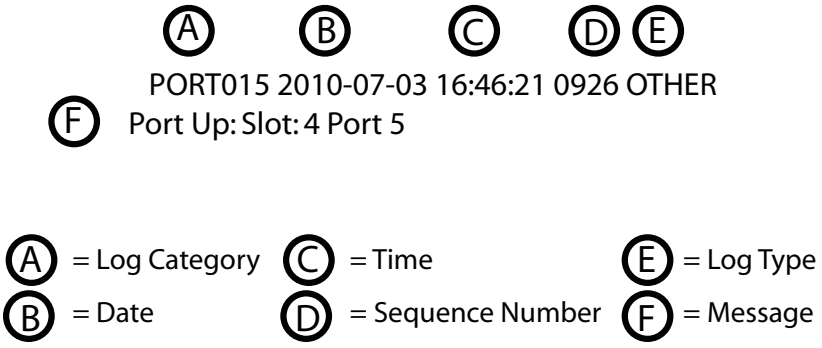

A B C D E
PORT015 2010-07-03 16:46:21 0926 OTHER
F Port Up: Slot: 4 Port 5
A = Log Category
B = Date
C = Time
D = Sequence Number
E = Log Type
F = Message

FIGURE 1-5 **Other logs**

4 Log Message Reference

This Log Message Reference lists the trap-associated logs and uses the following attributes:

- Category - These are explained in Section 1 and include the number within the category. NMS messages have the category NMS.
- Type - The types possible are FAULT, OTHER, INFO, and PROGRESS INDICATOR. For the NMS, the type is the associated configuration area (such as Discovery).
- Trap Text - This is the message passed with the log; these are listed in the NMS trap parser.
- Severity - These are critical, major, minor, and warning.
- Log Message - This is the descriptive text string that specifies the problem, and may include variables that identify a specific component.
- Reason Code - This can further identify the problem.
- Overview - This explains the scope of the problem and the possible faulty components.

The log messages are listed by Category, Reason Code, and Trap Text. Reading the logs with these attributes allows the user to quickly find the log in this table.

5 Network Loops

Network loops may be indicated by service degradations, connectivity problems on a link(s), etc. If the user suspects the presence of a network loop, they should attempt to find the loop and correct it. Some things that the user should look at are recent port and interface provisioning, recent EPSR provisioning, recent STP provisioning, and recent wiring and connections made within their network or connections external to their network.

2. SBx3112 Logs with Traps

1 Overview

This section lists the logs that apply to the SBx3112 product only. For logs that apply to both the SBx3112 and iMAP devices, refer to the Section 3.

1.1 Listing of Logs and Traps

This is a table that lists the log category / trap text that is the entry point for log descriptions. Each entry is a live link to the section that includes all of the reason codes.

1.2 Log and Trap Listing by Reason Code

This includes an overview of the log category / trap text and then a description for each Reason Code. For each Reason Code there are the following attributes:

- Message
- Severity
- Explanation
- Action
- Alarms - This is a list of components that can have alarms produced, and included here are any special notes because of the component type.

2 Listing of Logs and Traps

Use the following table to locate the Log Category and then the specific Reason Code

TABLE 2-1 Logs and Traps for the SBx3112

Log and Trap Text	Reason Code
CARD005 - atnCardDefectRaised	1.0v Power Failed 2.5V Power Failure 3.3v Power Failed (Mate) Control Link Lost Control Link Lost (CM side: slot 4) or (CM side: slot 5) Control Link Lost (SM side: slot 4) or (SM side: slot 5) Datalink Lost (CM Side: Link <A or B> Slot <4 or 5>) Datalink Lost (SM Side: Link <A or B> Slot <4 or 5>) High Temperature POE Power Requested Exceeds Card Power Limit PSE Device Fault PSE High Temp Detected PSE Power Failed SD Card Failed USB Failed
CARD044 - Not Applicable	Not Applicable
CARD045 - Not Applicable	Not Applicable
LOG005 - atnMediaLogStreamError	I/O error writing to media card Media card deactivated Media card not present

TABLE 2-1 **Logs and Traps for the SBx3112**

Log and Trap Text	Reason Code
PORT003 - atnPortDefectRaised	Insufficient Shelf PoE Power
	PD Overload
	PD Short Circuit
	PD Thermal Protection
	PD Underload Detected
	POE Device Fault
PORT005 - atnPortDefectRaised	Insufficient Card PoE Power
	MAC Thrashing Limit Exceeded
PSU001 - atnPSUFaultRaised	PSU Card Not Present
	PSU General Fault
	PSU Hardware Not Recognized
	PSU High Temperature
	PSU Input Voltage Fault
	PSU No Communication
	PSU Output Voltage Fault
SHLF001 - atnShelfFaultRaised	POE Usage Exceeds Power Threshold

2.1 CARD005 - atnCardDefectRaised

2.1.1 1.0v Power Failed

Message Card Failure Raised

Severity Critical

Explanation A problem has been detected with the 1.0v power output on the CFC200, affecting data packet processing. The CFC200 card is probably defective.

Action Perform the following:

1. Replace the CFC card. If the problem is still not resolved, contact Allied Telesis Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC200	Degraded	Critical
•	CFC200	Failed	Major

Note: For a simplex system, the alarm is critical since all data traffic could be dropped.

2.1.2 2.5V Power Failure

Message 2.5V Power Failure

Severity Critical

Explanation A problem has been detected with the 2.5v power output on the CFC200, affecting data packet processing. The CFC200 card is probably defective.

Action Perform the following:

1. Replace the CFC card. If the problem is still not resolved, contact Allied Telesis Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC200	Degraded	Critical
•	CFC200	Failed	Major

Note: For a simplex system, the alarm is critical since all data traffic could be dropped.

2.1.3 3.3v Power Failed

Message Card Failure Raised

Severity Critical

Explanation A problem has been detected with the 3.3v power output on the CFC12 or CFC200 card. The card is probably defective.

Action Perform the following:

1. Replace the CFC card. If the problem is still not resolved, contact Allied Telesis Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC12	Degraded	Critical
•	CFC200	Degraded	Critical
•	CFC200	Failed	Major

Note: For a simplex system, the alarm is critical since all data traffic could be dropped.

2.1.4 (Mate) Control Link Lost

Message To Be Supplied

Severity Major

Explanation The internal control links between the CFCs are Ethernet based, and so there is a condition defined that indicates the loss of control plane links between CFCs. This alarm can be discovered by either CFC in a duplex system.

Action Perform the following:

1. If the CFC slot is the active CFC, wait until a low traffic period and perform a switch of activity. Then perform the following steps that are for an inactive CFC. Perform the next step only if the current step does not resolve the problem.
2. Restart the inactive CFC
3. Reseat the inactive CFC.
4. Replace the inactive CFC.
5. If this does not resolve the problem, contact Allied Telesis support.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC200	Online	Major
•	GE24POE	Failed	Major
•	GE24SFP	Failed	Major
•	XE4	Failed	Major

Note: The inactive CFC is in a FAILED state, and so the card can be replaced without a further loss of traffic capacity.

2.1.5 Control Link Lost (CM side: slot 4) or (CM side: slot 5)

Message To Be Supplied

Severity Major

Explanation There is a control (messaging) link between each SM and each CFC (one control link to the CFC in slot 4 another control link to the CFC in slot 5). The CM runs a polling audit on the link, so if communication is lost, the CM will report this and will include which link (to slot 4 or 5). If the link is to the inactive CFC, layer 1 is lost, but switching traffic may not be affected.

Action Perform the following:

1. If the CFC slot is the active CFC, wait until a low traffic period and perform a switch of activity. Then perform the following steps that are for an inactive CFC. Perform the next step only if the current step does not resolve the problem.
2. Restart the SM.
3. Reseat the SM.
4. Restart the inactive CFC
5. Reseat the inactive CFC.
6. Replace the SM.
7. Replace the inactive CFC.
8. If this does not resolve the problem, contact Allied Telesis support.

Alarms The following components are affected:

	Component	Status	Alarm
•	XE4	Degraded	Major
•	GE24POE	Degraded	Major
•	GE24SFP	Degraded	Major

2.1.6 Control Link Lost (SM side: slot 4) or (SM side: slot 5)

Message To Be Supplied

Severity Major

Explanation There is a control (messaging) link between each SM and each CFC (one control link to the CFC in slot 4 and another control link to the CFC in slot 5). The SM runs a polling audit on the link, and if a control link is lost, the SM will report and include which slot (4 or 5). If the link is to the inactive CFC, layer 1 is lost, but switching traffic may not be affected. Also, if the control link lost is to the active CFC, the CFC will reboot the SM to try to resolve the problem.

Action Perform the following:

1. If the CFC slot is the active CFC, wait until a low traffic period and perform a switch of activity. Then perform the following steps. Perform the next step only if the current step does not resolve the problem.
2. Restart the SM.
3. Reseat the SM.
4. Restart the inactive CFC
5. Reseat the inactive CFC.
6. Replace the SM.
7. Replace the inactive CFC.

8. If this does not resolve the problem, contact Allied Telesis support.

Alarms The following components are affected:

	Component	Status	Alarm
•	XE4	Degraded	Major
•	GE24POE	Degraded	Major
•	GE24SFP	Degraded	Major

2.1.7 Datalink Lost (CM Side: Link <A or B> Slot <4 or 5>)

Message Card Failure Raised

Severity Major

Explanation There are two data (traffic) links between each SM and each CFC (two data links, A and B, to the CFC in slot 4, and two data links, A and B, to the CFC in slot 5). The CM runs a polling audit on the links, and if communication is lost, the CM will report this and the message will include which link (A or B) and which slot (4 or 5) has been lost. If the link is to the inactive CFC, layer 1 is lost, but switching traffic may not be affected.

Action Perform the following:

1. If the CFC slot is the active CFC, wait until a low traffic period and perform a switch of activity. Then perform the following steps. Perform the next step only if the current step does not resolve the problem.
2. Restart the SM.
3. Reseat the SM.
4. Restart the inactive CFC
5. Reseat the inactive CFC.
6. Replace the SM.
7. Replace the inactive CFC.
8. If this does not resolve the problem, contact Allied Telesis support.

Alarms The following components are affected:

	Component	Status	Alarm
•	XE4	Degraded	Major
•	GE24POE	Degraded	Major
•	GE24SFP	Degraded	Major

2.1.8 Datalink Lost (SM Side: Link <A or B> Slot <4 or 5>)

Message Card Failure Raised

Severity Major

Explanation There are two data (traffic) links between each SM and each CFC (two data links, A and B, to the CFC in slot 4 two data links, A and B, to the CFC in slot 5). The SM runs an interrupt audit on the links, and if communication is lost, the SM will report this and the message will include which link (A or B), and which slot (4 or 5) has been lost. If the link is to the inactive CFC, layer 1 is lost, but switching traffic may not be affected.

Action Perform the following:

1. If the CFC slot is the active CFC, wait until a low traffic period and perform a switch of activity. Then perform the following steps. Perform the next step only if the current step does not resolve the problem.
2. Restart the SM.
3. Reseat the SM.
4. Restart the inactive CFC
5. Reseat the inactive CFC.
6. Replace the SM.
7. Replace the inactive CFC.
8. If this does not resolve the problem, contact Allied Telesis support.

Alarms The following components are affected:

	Component	Status	Alarm
•	XE4	Degraded	Major
•	GE24POE	Degraded	Major
•	GE24SFP	Degraded	Major

2.1.9 High Temperature

Message To Be Supplied

Severity Major

Explanation The temperature sensor on the CFC200 has detected a temperature above 70 degrees Celsius.

Action Perform the following:

1. Input SHOW SYSTEM COOLING to see which components have had a temperature change and the status of the FM4.
2. Check the affected component and replace if necessary.

3. If multiple components are showing a temperature change, check the FM4 and replace if necessary.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC200	Degraded	Critical
•	CFC200	Failed	Critical

Note: In a simplex system, the CFC200 will be in a DEGRADED state, but will not go out of service, since traffic would be affected.

2.1.10 POE Power Requested Exceeds Card Power Limit

Message To Be Supplied

Severity Minor

Explanation The GE24POE card cannot support the POE current configuration. You must reconfigure the POE port power limits or add (if relevant) a PoE PSU. This card alarm informs whether or not more power could be requested than is available, even if no port is actually down. It is a warning that there is a risk for insufficient power alarms on the ports.

Action Perform the following:

1. Reconfigure the POE port power limits or add (if relevant) a PoE PSU.

Alarms The following components are affected:

	Component	Status	Alarm
•	GE24POE	Degraded	Minor

2.1.11 PSE Device Fault

Message To Be Supplied

Severity Major

Explanation A GE24POE card fault has been detected.

Action Perform the following:

1. Check the card and replace if necessary.

Alarms The following components are affected:

	Component	Status	Alarm
•	GE24POE	Degraded	Major

2.1.12 PSE High Temp Detected

Message To Be Supplied

Severity Major

Explanation The GP24POE card has exceeded the temperature threshold. Service could be affected.

Action Perform the following:

1. Check the card and replace the GE24POE card.

Alarms The following components are affected:

	Component	Status	Alarm
•	GE24POE	Degraded	Major

2.1.13 PSE Power Failed

Message To Be Supplied

Severity Major

Explanation The GP24POE card no longer has power to supply the POE subscriber lines.

Action Perform the following:

1. Replace the card.

Alarms The following components are affected:

	Component	Status	Alarm
•	GE24POE	N/A	Major

2.1.14 SD Card Failed

Message Card Failure Raised

Severity Major

Explanation The SD card in the active CFC200 has failed, and so cannot written in or copied out.

Action Perform the following:

1. Activate and deactivate the SD card.
2. Replace the SD card.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC200	Online	Major
•	CFC200	Online	Major

2.1.15 USB Failed

Message To Be Supplied

Severity Major

Explanation The USB in the active CFC200 has failed, and so files cannot be written in or copied out.

Action Perform the following:

1. Replace the USB device.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC200	Online	Major
•	CFC200	Online	Major

2.2 CARD044 - Not Applicable

2.2.1 Not Applicable

Message Media Card State Change

Severity Info

Explanation A media card (e.g.,compact flash card) has changed operational state. The state change could be the result of the card being physically inserted or removed, or could be the result of the card being activated or deactivated by a user via CLI commands.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	None		

2.3 CARD045 - Not Applicable

2.3.1 Not Applicable

Message Media Card Diagnostics Failure

Severity Info

Explanation A media card (e.g., compact flash card) has failed out of service diagnostics. The card is most likely faulty or not inserted correctly, or there is a problem with the CFC24 it is plugged in to.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.4 LOG005 - atnMediaLogStreamError

2.4.1 I/O error writing to media card

Message Failed to write management logs to storage media

Severity Major

Explanation The user has configured log streaming to a media card, but streaming can no longer occur because the card is full or is no longer present.

Action Perform the following:

1. Re-insert the media card or remove files.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.4.2 Media card deactivated

Message Failed to write management logs to storage media

Severity Major

Explanation The user has deactivated this media unit. It won't be available for use again until it is activated.

Action Perform the following:

1. Activate the media card

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.4.3 Media card not present

Message Failed to write management logs to storage media

Severity Major

Explanation The user has configured log streaming to a media card, but streaming can no longer occur because the card is no longer present. The media card has been extracted from the unit.

Action Perform the following:

1. Insert the media card back into the CFC200.

Alarms The following components are affected:

	Component	Status	Alarm
•	None		

2.5 PORT003 - atnPortDefectRaised

2.5.1 Insufficient Shelf PoE Power

Message To Be Supplied

Severity Major

Explanation There is not enough power to supply the GE24POE configuration.

Action Perform the following:

1. Either add a PSU (if only is configured) or lower port power limits

Alarms The following components are affected:

	Component	Status	Alarm
•	Shelf	N/A	Minor

2.5.2 PD Overload

Message To Be Supplied

Severity Major

Explanation A subscriber device has overloaded the power capacity of the port.

Action Perform the following:

1. Replace the PD.

Alarms The following components are affected:

	Component	Status	Alarm
•	GE24POE Port	Degraded	Major

2.5.3 PD Short Circuit

Message To Be Supplied

Severity Major

Explanation A subscriber device has caused a short circuit.

Action Perform the following:

1. Replace the PD.

Alarms The following components are affected:

	Component	Status	Alarm
•	GE24POE Port	Degraded	Major

2.5.4 PD Thermal Protection

Message To Be Supplied

Severity Major

Explanation A port on the GP24POE card has had to throttle back its power because of the temperature.

Action Perform the following:

1. Replace the PD.

Alarms The following components are affected:

	Component	Status	Alarm
•	GE24POE Port	Degraded	Major

2.5.5 PD Underload Detected

Message To Be Supplied

Severity Major

Explanation The PD (Powered Device) is not drawing as much current as expected.

Action Perform the following:

1. Replace the PD.

Alarms The following components are affected:

	Component	Status	Alarm
•	GE24POE Port	Degraded	Major

2.5.6 POE Device Fault

Message To Be Supplied

Severity Major

Explanation There is a fault on the subscriber end.

Action Perform the following:

1. Replace equipment at the subscriber end.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.6 PORT005 - atnPortDefectRaised

2.6.1 Insufficient Card PoE Power

Message To Be Supplied

Severity Major

Explanation There is not enough power to supply the GE24POE configuration.

Action Perform the following:

1. Either add a PSU (if only one is configured) or lower port power limits.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.6.2 MAC Thrashing Limit Exceeded

Message To Be Supplied

Severity Minor

Explanation Any time a MAC move occurs, it is considered a potential duplicate address. When the first MAC move is detected a system-wide one second timer starts. During this second, the MAC move count increments. For inter-card interfaces, if the count exceeds 128 before the second expires, a duplicate address condition is declared and the interface on which the next MAC move occurs is learning disabled. Packets received will continue to forward. For intra-card interfaces the interface is learning disabled immediately and will stay in a learning disabled state for 60 seconds. A PORT007 log (INFO) is also produced showing the port state change from UP-UP-Online to UP-UP-Degraded.

Action Perform the following:

1. Check for network loops, since that is probably the cause of the log.
2. If the command SET SWITCH MACREMOVALMODE=AGEONLY has been issued, and a cable that handles a large number of devices is physically moved from one port to another, the device MAC addresses will naturally appear on the new port and will be detected by the MAC Thrash Limiting feature. This could trigger the alarm.

Alarms The following components are affected:

Component	Status	Alarm
• GE Port	Degraded	Major
• XE Port	Degraded	Major

2.7 PSU001 - atnPSUFaultRaised

2.7.1 PSU Card Not Present

Message PSU Failure Raised

Severity Major

Explanation One of the PSU units is not present in the shelf. The shelf can continue to function but there is no backup if the remaining unit fails.

Action Perform the following:

1. Replace the PSU.

Alarms The following components are affected:

	Component	Status	Alarm
•	PSU	Failed	Major

2.7.2 PSU General Fault

Message PSU Failure Raised

Severity Major

Explanation This is a generic PSU Fault alarm that has the same severity and state impact as the other PSU alarms, and covers alarms not reported by the other PSU alarms, usually Fan Failure. The action like other PSU faults is to replace the card or place the PSU in the correct slot.

Action Perform the following:

1. Replace the card or place the PSU in the correct slot.

Alarms The following components are affected:

	Component	Status	Alarm
•	PSU	Failed	Major

2.7.3 PSU Hardware Not Recognized

Message PSU Failure Raised

Severity Major

Explanation A PoE PSU is already installed in one PoE PSU slot and a System PSU has been installed in the other PoE PSU slot. (A No Communication log is also output.)

Action Perform the following:

- Remove the System PSU and place it in the correct slot.

Alarms The following components are affected:

Component	Status	Alarm
• PSU	Failed	Major

2.7.4 PSU High Temperature

Message PSU Failure Raised

Severity Major

Explanation This is caused when the temperature sensor on the PSU detects a temperature above 50 degrees Celsius, and puts the PSU into a Failed state.

Action Perform the following:

1. Input SHOW SYSTEM COOLING to see which components have had a temperature change and the status of the FM4.
2. Check the affected component and replace if necessary.
3. If multiple components are showing a temperature change, check the FM4 and replace if necessary.

Alarms The following components are affected:

Component	Status	Alarm
• PSU	Failed	Major

2.7.5 PSU Input Voltage Fault

Message PSU Failure Raised

Severity Major

Explanation The POE PSU has been incorrectly placed in a SYS POE slot (C or D).

Action Perform the following:

1. Remove the PSU and place it in the correct POE (A or B) slot.

Note: It is also possible that the power is disconnected; in that case you will have both the Input Voltage Fault and Output Voltage Fault alarms. Connect the power.

Alarms The following components are affected:

Component	Status	Alarm
• PSU	Failed	Major

2.7.6 PSU No Communication

Message PSU Failure Raised

Severity Major

Explanation A PoE PSU has been installed in one PoE PSU slot and a System PSU is installed in the other PoE PSU slot. (A Hardware Not Recognized log is also output.)

Action Perform the following:

1. Remove the System PSU from the POE (A or B) slot and place it in the correct slot (C or D).

Alarms The following components are affected:

	Component	Status	Alarm
•	PSU	Failed	Major

2.7.7 PSU Output Voltage Fault

Message PSU Failure Raised

Severity Major

Explanation The POE PSU has been incorrectly placed in a SYS PSU slot (C or D).

Action Perform the following:

- Remove the PSU and place it in the correct POE (A or B) slot.

Alarms The following components are affected:

	Component	Status	Alarm
•	PSU	Failed	Major

2.8 SHLF001 - atnShelfFaultRaised

2.8.1 POE Usage Exceeds Power Threshold

Message To Be Supplied

Severity Info

Explanation The power thresholds that have been set have been exceeded.

Action Perform the following:

1. Add a PSU (if applicable) or remove PoE interfaces.

Alarms The following components are affected:

	Component	Status	Alarm

•	Shelf	Degraded	Info

3. Allied Telesis Product Logs with Traps

1 Overview

This section is organized as follows.

1.1 Listing of Logs and Traps

This is a table that lists the log category / trap text that is the entry point for log descriptions. Each entry is a live link to the section that includes all of the reason codes.

1.2 Log and Trap Listing by Reason Code

This includes an overview of the log category / trap text and then a description for each Reason Code. For each Reason Code there are the following attributes:

- Message
- Severity
- Explanation
- Action
- Alarms - This is a list of components that can be affected, and includes any special notes because of the component type.

2 Listing of Logs and Traps

The following table lists the common logs and trap text that apply to the SBx3112 as well as other Allied Telesis NSP products.

TABLE 3-1 Logs and Traps for SBx3112

Log and Trap Text	Reason Code (or Message)
CARD001 - entConfigChangeTrap	Card Mismatch
CARD003 - atnCardDefectRaised	Card Not Present
CARD005 - atnCardDefectRaised	ARP Filtering Configuration Failed ARP Filtering Configuration Not Supported ARP Filtering Resources Exceeded Boot Failed Card Diags Failed Config Failed Diags Failed Failed to Access Card Heartbeat Lost Load Card Failed QOS Configuration Failed QOS Configuration Not Supported QOS Resources Exceeded Rate Limiting Failed Reset Failed RTC Battery Simplex Software Version Compatibility Unable to Access Card
CARD023 - atnCardDefectRaised	Database in Upgrade Mode File Corruption Inconsistent Load McastGroupLimit Out of Sync

TABLE 3-1 **Logs and Traps for SBx3112**

Log and Trap Text	Reason Code (or Message)
CARD043 - Not Applicable	Not Applicable
CFCP001 - atnRedundancyLost	Not Applicable
CFCP002 - atnRedundancyRestored	Unknown
CFCP014 - atnEpsrNodeTrap	Not Applicable
CHAS001 - entConfigChangeTrap	Not Applicable
FAN001 - atnFanFaultRaised	Fan Module Not Present Fans Not Rotating Properly Hardware Not Recognized High Temperature No Communication
IGMP000 - mcHighWaterMarkPerCardExceeded	Not Applicable
IGMP001 - mcChannelLimitPerShelfExceeded	Not Applicable
IGMP002 - mcHighWaterMarkPerCardCleared	Not Applicable
IGMP003 - mcGroupLimitPerMACExceeded	Not Applicable
IGMP004 - mcMACLimitPerPortExceeded	Not Applicable
IGMP005 - mcFirstRouterDetected	Not Applicable
IGMP006 - mcNewRouterDetected	Not Applicable
IGMP007 - mcLastRouterAgedOut	Not Applicable
IGMP008 - mcRouterAgedOut	Not Applicable
IGMP009 - (no Trap Message)	Not Applicable
IGMP010 - (no Trap Message)	Not Applicable

TABLE 3-1 **Logs and Traps for SBx3112**

Log and Trap Text	Reason Code (or Message)
INTF003 - (no Trap Message)	Classifier Configuration Failed Classifier Configuration Not Supported Classifier Resources Exceeded
IPIF001 - (To Be Supplied)	IP Interface Configuration Failed
LOG005 - atnMediaLogStreamError	I/O error writing to compact flash Compact flash unit deactivated Compact flash media not present
LOG006 - Not Applicable	Not Applicable
PORT003 - Linkdown	BFD Detected Miswiring BFD Session Failed Config Failed Disable Failed Enable Failed Loss of Frame (LOF) Loss of Link (LOL) Loss of Signal (LOS) Loss of Sync (LOSY) Remote BFD Session Failed Reset Failed SFP Not Present Unexpected BPDU Received XFP Not Present
PORT005 - atnPortDefectRaised	Classifier Configuration Failed Classifier Configuration Not Supported Classifier Resources Exceeded
RMON001 - risingAlarm	Not Applicable
RMON002 - fallingAlarm	Not Applicable
SHLF001 - atnShelfFaultRaised	Port Outage Threshold VLAN has no NETWORK facing interface

TABLE 3-1 **Logs and Traps for SBx3112**

Log and Trap Text	Reason Code (or Message)
SYS004 - atnCardDefectRaised	Database Audit Failure Database Transaction Failure Death of non-critical task Flash Write Failure
SYS009 - atnShelfFaultRaised	Cannot Read MAC Address
TRAP003 - coldStartTrap	Not Applicable
TRAP004 - warmStart	Not Applicable
TRAP009 - entConfigChangeTrap	Not Applicable

2.1 CARD001 - entConfigChangeTrap

2.1.1 Card Mismatch

Message `Card Mismatch Raised`

Severity `Major`

Explanation `The card currently in the slot does not match the provisioning data associated with the slot. As a result, it is not possible to bring the card in-service.`

Action `Perform the following:`

1. Ensure the card is installed in a valid slot.
2. Replace the card with a card of the correct type or remove the existing provisioning data and reprovision based on the card that is present.

Alarms `The following components are affected:`

Component	Status	Alarm
• ADSL	Not installed	Minor
• CES8	Not installed	Major
• CFC200	Not Installed	Major
• CFC24	Not installed	Minor
• CFC6	Not installed	Minor
• EPON2	Not installed	Major
• FE10	Not installed	Minor

• FX10	Not installed	Minor
• GE Card	Not installed	Major
• GE24POE	Not Installed	Major
• GE24SFP	Not Installed	Major
• NTE8	Not Installed	Major
• POTS24	Not installed	Minor
• SHDSL24	Not Installed	Minor
• XE Card	Not installed	Major
• XE4	Not Installed	Major

Note: For the CFC200, when the inactive is UP-DN for any reason it is a Major alarm because of the shared switch fabrics; bandwidth is lost in this condition, which is different from iMAP CFCs (Minor).

Note: For both iMAP and SBx3112, GE and XE interfaces have an UP/DOWN severity of Major.

2.2 CARD003 - atnCardDefectRaised

2.2.1 Card Not Present

Message `Card Not Present Raised`

Severity `Major`

Explanation `A configured card is no longer present in the specified slot or the card has been removed from the system.`

Action `Perform the following:`

1. Take the absent card out of service (quiet the alarm) or insert a card of the type that matches the provisioning remove the card provisioning.

Alarms `The following components are affected:`

Component	Status	Alarm
• ADSL	Not installed	Minor
• CES8	Not installed	Major
• CFC200	Not Installed	Major
• CFC24	Not installed	Minor
• CFC6	Not installed	Minor
• EPON2	Not installed	Major
• FE10	Not installed	Minor

• FX10	Not installed	Minor
• GE Card	Not installed	Major
• GE24POE	Not Installed	Major
• GE24SFP	Not Installed	Major
• NTE8	Failed	Major
• POTS24	Not installed	Minor
• SHDSL24	Online	Minor
• XE Card	Not installed	Major
• XE4	Not Installed	Major

Note: For both iMAP and SBx3112, GE and XE interfaces have an UP/DOWN severity of Major.

2.3 CARD005 - atnCardDefectRaised

2.3.1 ARP Filtering Configuration Failed

Message `Card Failure Raised`

Severity `Minor`

Explanation `The reported card rejected the provisioned ARPFILTER setting for ports on the card due to unspecified reasons. ARPFILTER functionality may not behave correctly.`

Action `Perform the following:`

1. Check the ARPFILTER settings.

Alarms `The following components are affected:`

Component	Status	Alarm
• ADSL	Failed	Minor
• FE10	Failed	Minor
• FE2	Failed	Minor
• FX10	Failed	Minor
• GE Card	Failed	Major
• GE Virtual Card	Failed	Major
• GE24POE	Failed	Major
• GE24SFP	Failed	Major
• NTE8	Failed	Major

• SHDSL24	Failed	Minor
• XE Card	Failed	Major
• XE4	Failed	Major

Note: Any time there is a card failure on the GE8 the alarm level is major due to service impact.

2.3.2 ARP Filtering Configuration Not Supported

Message `Card Failure Raised`

Severity `Minor`

Explanation `The reported card is not capable of supporting the provisioned ARP-FILTER setting for ports on the card. This may be due to the reported card running an older software revision. ARPFILTER functionality may not behave correctly.`

Action `Perform the following:`

1. To Be Supplied

Alarms `The following components are affected:`

Component	Status	Alarm
• ADSL	Failed	Minor
• FE10	Failed	Minor
• FE2	Failed	Minor
• FX10	Failed	Minor
• GE Card	Failed	Major
• GE Virtual Card	Failed	Major
• GE24POE	Failed	Major
• GE24SFP	Failed	Major
• NTE8	Failed	Major
• SHDSL24	Failed	Minor
• XE Card	Failed	Major
• XE4	Failed	Major

2.3.3 ARP Filtering Resources Exceeded

Message `Card Failure Raised`

Severity `Minor`

Explanation The reported card has insufficient resources to support the provisioned ARPFILTER setting for ports on the card. ARPFILTER functionality may not behave correctly.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• ADSL	Failed	Minor
• FE10	Failed	Minor
• FE2	Failed	Minor
• FX10	Failed	Minor
• GE Card	Failed	Major
• GE Virtual Card	Failed	Major
• GE24POE	Failed	Major
• GE24SFP	Failed	Major
• NTE8	Failed	Major
• SHDSL24	Online	Minor
• XE Card	Failed	Major
• XE4	Failed	Major

2.3.4 Boot Failed

Message Card Failure Raised

Severity Major

Explanation The card failed to boot a software load from it's flash memory into its RAM memory. The problem could be with the file on the card's FLASH, or the card itself may be defective.

Action Perform the following:

1. Verify the load file preference settings.
2. Disable/enable the card.
3. Disable the card, load the card manually using PUT FILE, then enable the card again.
4. Disable the card, reseat the card, enable it again.
5. Disable the card, replace the card, enable it again.

Alarms The following components are affected:

Component	Status	Alarm

• ADSL	Failed	Minor
• CES8	Failed	Major
• EPON2	Failed	Major
• FE10	Failed	Minor
• FX10	Failed	Minor
• GE Card	Failed	Major
• GE24POE	Failed	Major
• GE24SFP	Failed	Major
• NTE8	Failed	Major
• POTS24	Failed	Minor
• SHDSL24	Online	Minor
• XE4	Failed	Major

2.3.5 Card Diags Failed

Message Card Failure Raised

Severity Major

Explanation The card failed diagnostic testing. The card is probably defective.

Action Perform the following:

1. Replace the card.

Alarms The following components are affected:

Component	Status	Alarm
• GE Card	Failed	Major
• GE Virtual Card	Failed	Major
• GE24POE	Failed	Major
• GE24SFP	Failed	Major
• XE Card	Failed	Major
• XE4	Failed	Major

2.3.6 Config Failed

Message Card Failure Raised

Severity Major

Explanation The card failed to configure properly. The card could be running an incorrect load that does not support the provisioning, there could

be a problem with provisioning associated with the card, or the card may be defective.

Action Perform the following:

1. Verify the load file preference settings.
2. Verify the provisioning data.
3. Disable and enable the card again.
4. Disable the card, reseat the card, enable it again.
5. Disable the card, replace the card, enable it again.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL	Failed	Minor
•	CES8	Failed	Major
•	CFC200	Failed	Major
•	EPON2	Failed	Major
•	FE10	Failed	Minor
•	FE2	Failed	Minor
•	FX10	Failed	Minor
•	GE24POE	Failed	Major
•	GE24SFP	Failed	Major
•	NTE8	Failed	Major
•	POTS24	Failed	Minor
•	SHDSL24	Online	Minor
•	XE Card	Failed	Major
•	XE4	Failed	Major

2.3.7 Diags Failed

Message Card Info Alarm Raised

Severity Major

Explanation The card failed diagnostic testing. The card is probably defective.

Action Perform the following:

1. If the active CFC for duplex system, switch activity and replace the card during a low-traffic period.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL	Failed	Minor
•	CES8	Failed	Major
•	CFC12	Degraded	Critical
•	CFC200	Degraded	Critical
•	CFC200	Failed	Major
•	CFC24	Degraded	Critical
•	CFC24	Failed	Minor
•	CFC4	Degraded	Critical
•	CFC6	Degraded	Critical
•	CFC6	Failed	Minor
•	EPON2	Failed	Major
•	FE10	Failed	Minor
•	FE2	Failed	Minor
•	FX10	Failed	Major
•	NTE8	Failed	Major
•	POTS24	Failed	Minor
•	SHDSL24	Failed	Minor

Note: For an active CFC, resolve immediately. Switch activity to mate CFC if it is available and has no corresponding alarm.

2.3.8 Failed to Access Card

Message `Card Failure Raised`

Severity `Minor`

Explanation `The control module failed to communicate with the specified card during some maintenance activity. The problem could be due to high traffic running through the card that exceeds it processing capacity. The problem could also be with card seating, or the card may be defective.`

Action `Perform the following:`

1. Reseat the card.
2. Run diagnostics on the card, and replace if necessary.

Alarms `The following components are affected:`

Component	Status	Alarm

• ADSL	Failed	Minor
• CES8	Failed	Major
• CFC200	Failed	Major
• CFC24	Failed	Minor
• CFC6	Failed	Minor
• EPON2	Failed	Major
• FE10	Failed	Minor
• FE2	Failed	Minor
• FX10	Failed	Minor
• GE Card	Failed	Major
• GE Virtual Card	Failed	Major
• GE24POE	Failed	Major
• GE24SFP	Failed	Major
• NTE8	Failed	Major
• POTS24	Failed	Minor
• SHDSL24	Online	Minor
• XE Card	Failed	Major
• XE4	Failed	Major

2.3.9 Heartbeat Lost

Message	Card Failure Raised
Severity	Minor
Explanation	The card failed a routine heartbeat check, where the control module attempts to verify message communication with the card. The problem could be due to high traffic running through the card that exceeds it's processing and messaging capacity. The problem could also be due to a software exception in the card.
Action	Perform the following: 1. Disable the card and enable card. 2. Replace card if necessary. For simplex systems, replace the card. 3. For duplex systems, swap activity, then replace the faulty card. 4. If the problem is still not resolved, contact Allied Telesis Support.
Alarms	The following components are affected:

	Component	Status	Alarm
•	ADSL	Failed	Minor
•	CES8	Failed	Major
•	CFC200	Failed	Major
•	CFC24	Failed	Minor
•	CFC6	Failed	Minor
•	EPON2	Failed	Major
•	FE10	Failed	Minor
•	FX10	Failed	Minor
•	GE Card	Failed	Major
•	GE Virtual Card	Failed	Minor
•	GE24POE	Failed	Major
•	GE24SFP	Failed	Major
•	NTE8	Failed	Major
•	POTS24	Failed	Minor
•	SHDSL24	Online	Minor
•	XE Card	Failed	Major
•	XE4	Failed	Major

2.3.10 Load Card Failed

Message `Card Failure Raised`

Severity `Major`

Explanation The system failed in an attempt to transfer a software load file from the control module to the card's flash memory. The card may have defective flash memory, or there could be a problem with the load file itself.

Action Perform the following:

1. Verify load file existence using SHOW FILES, and fix if necessary.
2. Verify load file integrity using AUDIT FILES, and fix if necessary.
3. Disable/enable card again.
4. Disable card, load the card manually using PUT FILE, then enable the card again.
5. Disable the card, reseat the card, enable it again.
6. Disable the card, replace the card, enable it again.

Alarms The following components are affected:

Component	Status	Alarm
• ADSL	Failed	Minor
• CES8	Failed	Major
• CFC12	Failed	Minor
• CFC200	Failed	Major
• EPON2	Failed	Major
• FE10	Failed	Minor
• FX10	Failed	Minor
• GE Card	Failed	Major
• GE24POE	Failed	Major
• GE24SFP	Failed	Major
• NTE8	Failed	Major
• POTS24	Failed	Minor
• SHDSL24	Failed	Minor
• XE4	Failed	Major

2.3.11 QOS Configuration Failed

Message Card Failure Raised

Severity Minor

Explanation The user has pre-provisioned a system QoS setting (e.g. via SET VLANQUEUEMAP) that the reported card cannot support. This may be due to the reported card running an older software revision. System QoS functions may not behave correctly.

Action Perform the following:

1. Verify QOS provisioning.
2. Verify card load preferences.
3. Disable/enable card.

Alarms The following components are affected:

Component	Status	Alarm
• ADSL	Degraded	Minor
• CFC200	Degraded	Minor
• EPON2	Degraded	Major

• FE10	Degraded	Minor
• FE2	Degraded	Minor
• FX10	Degraded	Minor
• GE Card	Degraded	Minor
• GE Virtual Card	Degraded	Minor
• GE24POE	Degraded	Minor
• GE24SFP	Degraded	Minor
• NTE8	Degraded	Minor
• SHDSL24	Degraded	Minor
• XE Card	Degraded	Minor
• XE4	Degraded	Minor

2.3.12 QOS Configuration Not Supported

Message `Card Failure Raised`

Severity `Minor`

Explanation `The user has pre-provisioned a system QoS setting (e.g. via SET VLANQUEUEMAP) that the reported card cannot support. This may be due to the reported card running an older software revision. System QoS functions may not behave correctly.`

Action `Perform the following:`

1. Verify QOS provisioning.
2. Verify card load preferences.
3. Disable/enable card.

Alarms `The following components are affected:`

Component	Status	Alarm
• ADSL	Degraded	Minor
• CFC200	Degraded	Minor
• EPON2	Degraded	Major
• FE10	Degraded	Minor
• FE2	Degraded	Minor
• FX10	Degraded	Minor
• GE Card	Degraded	Minor
• GE Virtual Card	Degraded	Minor
• GE24POE	Degraded	Minor

• GE24SFP	Degraded	Minor
• NTE8	Degraded	Minor
• SHDSL24	Degraded	Minor
• XE Card	Degraded	Minor
• XE4	Degraded	Minor

2.3.13 QOS Resources Exceeded

Message `Card Failure Raised`

Severity `Minor`

Explanation `The user has pre-provisioned a system QoS setting (e.g. via SET VLANQUEUEMAP) that the reported card cannot support. This may be due to the reported card running an older software revision. System QoS functions may not behave correctly.`

Action `Perform the following:`

1. Verify QOS provisioning.
2. Verify card load preferences.
3. Disable/enable card.
4. If the problem is still not resolved, contact Allied Telesis Support.

Alarms `The following components are affected:`

Component	Status	Alarm
• ADSL	Degraded	Minor
• CFC200	Degraded	Minor
• EPON2	Degraded	Major
• FE10	Degraded	Minor
• FE2	Degraded	Minor
• FX10	Degraded	Minor
• GE Card	Degraded	Minor
• GE Virtual Card	Degraded	Minor
• GE24POE	Degraded	Minor
• GE24SFP	Degraded	Minor
• NTE8	Degraded	Minor
• SHDSL24	Degraded	Minor
• XE Card	Degraded	Minor

• XE4	Degraded	Minor

2.3.14 Rate Limiting Failed

Message `Card Failure Raised`

Severity `Minor`

Explanation `The reported card/interface has rejected the provisioned rate limiting value(s). Egress traffic from the interface(s) on the card may not be correctly limited.`

Action `Perform the following:`

1. Verify that the provisioned RATE and BURST values are supported by that type of interface.
2. Verify card load preferences show the most current software, if applicable.
3. Disable/enable card.
4. If the problem is still not resolved, contact Allied Telesis Support.

Alarms `The following components are affected:`

	Component	Status	Alarm
•	ADSL	Failed	Minor
•	FE10	Failed	Minor
•	FE2	Failed	Minor
•	FX10	Failed	Minor
•	GE Card	Failed	Major
•	GE Virtual Card	Failed	Major
•	GE24POE	Failed	Major
•	GE24SFP	Failed	Major
•	SHDSL24	Online	Minor
•	XE Card	Failed	Major
•	XE4	Failed	Major

2.3.15 Reset Failed

Message `Card Failure Raised`

Severity `Major`

Explanation `A software reset of the card failed. The card may be defective or not seated properly.`

Action `Perform the following:`

1. Disable/enable the card.
2. Reseat the card if necessary.
3. Replace the card if necessary.
4. If the problem is still not resolved, contact Allied Telesis Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL	Failed	Minor
•	ARP	Failed	Minor
•	CES8	Failed	Major
•	CFC200	Failed	Major
•	CFC24	Failed	Minor
•	CFC6	Failed	Minor
•	EPON2	Failed	Major
•	FE10	Failed	Minor
•	FX10	Failed	Minor
•	GE Card	Failed	Major
•	GE24POE	Failed	Major
•	GE24SFP	Failed	Major
•	NTE8	Failed	Major
•	POTS24	Failed	Minor
•	PPP	Failed	Minor
•	SHDSL24	Online	Minor
•	XE Port	Failed	Major
•	XE4	Failed	Major

Note: For the CFC200, this is for the inactive unit only.

2.3.16 RTC Battery

Message Card Failure Raised

Severity Major

Explanation The real time clock battery on the card is defective.

Action Perform the following:

1. For simplex systems, replace the CFC card.

2. For duplex systems, swap activity, then replace the faulty card.
3. If the problem is still not resolved, contact Allied Telesis Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC12	Degraded	Minor
•	CFC200	Degraded	Minor
•	CFC24	Degraded	Minor
•	CFC4	Degraded	Minor
•	CFC6	Degraded	Minor

Note: For this alarm, it is possible to swap CFCs.

2.3.17 Simplex

Message Card Info Alarm Raised

Severity Minor

Explanation The inactive Control Module is not online, so the system is running in simplex mode.

Action Perform the following:

1. If this is intentional, no action is required.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC200	N/A	Major
•	CFC24	Any	Minor
•	CFC6	Any	Minor

Note: Since the CFC200 works in load sharing mode, going to simplex means traffic could be affected.

2.3.18 Software Version Compatibility

Message Card Failure Raised

Severity Minor

Explanation The card's load preferences are set to a software load file whose version is not compatible with the particular type and version of card hardware.

Action Perform the following:

1. Verify load file preference settings. Most likely the load file doesn't match the card type.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL	Failed	Minor
•	CES8	Failed	Major
•	CFC200	Failed	Major
•	EPON2	Failed	Major
•	FE10	Failed	Minor
•	FX10	Failed	Minor
•	GE Card	Failed	Major
•	GE24POE	Failed	Major
•	GE24SFP	Failed	Major
•	NTE8	Failed	Major
•	POTS24	Failed	Minor
•	SHDSL24	Failed	Minor
•	XE4	Failed	Major

2.3.19 Unable to Access Card

Message Card Failure Raised

Severity Major

Explanation The control module failed to communicate with the specified card during some maintenance activity. The problem could be due to high traffic running through the card that exceeds it processing capacity. The problem could also be with card seating, or the card may be defective.

Action Perform the following:

1. If a CFC card, reseat the card. If this fails replace the card. If this fails, contact Allied Telesis Technical Support.
2. If this is an SM card, disable the card, and enable the card. If the alarm is still not cleared, Reseat the card. If the alarm is still not cleared, replace the card.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL	Failed	Minor
•	CES8	Failed	Major

• CFC200	Failed	Major
• CFC24	Failed	Minor
• CFC6	Failed	Minor
• EPON2	Failed	Major
• FE10	Failed	Minor
• FE2	Failed	Minor
• FX10	Failed	Minor
• GE Card	Failed	Major
• GE Virtual Card	Failed	Major
• NTE8	Failed	Major
• POTS24	Failed	Minor
• SHDSL24	Online	Minor
• XE Card	Failed	Major

2.4 CARD023 - atnCardDefectRaised

2.4.1 Database in Upgrade Mode

Message `Card Info Alarm Raised`

Severity `Info`

Explanation `A software upgrade is in progress. The alarm condition will be cleared and the LED extinguished once the upgrade is completed.`

Action `Perform the following:`

1. Commit to upgrade as per upgrade procedure.

Alarms `The following components are affected:`

Component	Status	Alarm
• CFC12	Online	Minor
• CFC200	Online	Minor
• CFC24	Online	Minor
• CFC24	Online	Minor
• CFC4	Online	Minor
• CFC6	Online	Minor

Note: You cannot swap the CFCs, since this is a normal part of an upgrade procedure.

2.4.2 File Corruption

Message Card Failure Raised

Severity Warning

Explanation A CRC calculation check has failed on one or more software load files that are resident in the flash memory of the specified control module card.

Action Perform the following:

1. Verify FLASH file integrity using the AUDIT FILES command and remove any corrupted files.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC12	Online	Info
•	CFC200	Online	Info
•	CFC24	Online	Info
•	CFC4	Online	Info
•	CFC6	Online	Info

2.4.3 Inconsistent Load

Message Card Failure Raised

Severity Info

Explanation The card is running a software version that does not match the software version running in the Control Module. As a result, some features may not function as expected.

Action Perform the following:

1. The card needs to have its software version upgraded to match the Control Module.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL Card	Online	Minor
•	CES8 card	Online	Major
•	EPON2	Online	Major
•	FE10 card	Online	Minor
•	FX10 Card	Online	Minor
•	GE Card	Online	Major

• GE Card	Online	Major
• GE24POE	Online	Major
• GE24SFP	Online	Major
• NTE8	Online	Major
• POTS24 Card	Online	Minor
• SHDSL24	Online	Minor
• XE4	Online	Major

2.4.4 McastGroupLimit

Message `Card Info Failure Raised`

Severity `Info`

Explanation `More IGMP Reports have been received on one Service Module than the provisioned slot's group limit (GRPLIMIT).`

Action `Perform the following:`

1. Verify traffic engineering for card.
2. Clear the alarm using CLEAR ALARMS command.

Alarms `The following components are affected:`

Component	Status	Alarm
• ADSL	Online	Info
• EPON2	Online	Info
• FE10	Online	Info
• FX10	Online	Info
• GE Card	Online	Info
• GE Virtual Card	Online	Info
• GE2	Online	Info
• NTE8	Online	Info
• SHDSL24	Online	Info
• XE Card	Online	Info

2.4.5 Out of Sync

Message `Card Info Alarm Raised`

Severity `Info`

Explanation The inactive Control Module has reached online status, but the data service protocols have not yet synchronized, therefore the system is not ready to support a swap of activity.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC200	Online	Info
•	CFC24	Online	Info
•	CFC6	Online	Info

2.5 CARD043 - Not Applicable

2.5.1 Not Applicable

Message Restart requested by OAM Audit Task

Severity Info

Explanation A routine audit process has discovered a card that is administratively enabled but in a failed operational state. The audit has initiated a restart on the card in an attempt to restore it to service.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	None		

2.6 CFCP001 - atnRedundancyLost

2.6.1 Not Applicable

Message Shelf Operating in simplex CFC mode

Severity Info

Explanation The system, configured for duplex mode, has dropped out of sync and is operating in the simplex mode.

Action Perform the following:

1. If this is expected, no action is required.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.7 CFCP002 - atnRedundancyRestored

2.7.1 Unknown

Message Shelf Operating in duplex CFC mode

Severity Info

Explanation The system, configured for duplex mode, has restored the inactive control module to service as hot standby. Both control modules are in sync and redundant operation is restored.

Explanation

Action Perform the following:

1. To Be Suppled

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.8 CFCP014 - atnEpsrNodeTrap

2.8.1 Not Applicable

Message (N/A)

Severity Master Node EPSR State Change

Explanation In an EPSR ring configuration, the master Node has undergone a state change. Possible states are: Idle, Completed, Failed.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.9 CHAS001 - entConfigChangeTrap

2.9.1 Not Applicable

Message Chassis Configuration Change

Severity Warning

Explanation A card in the chassis has been created or deleted.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

	Component	Status	Alarm
•	None		

2.10 FAN001 - atnFanFaultRaised

2.10.1 Fan Module Not Present

Message Fan Module Not Present

Severity Critical

Explanation The fan module is not present in the shelf.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	FM4	Not Installed	Major
•	FM8	Not Installed	Major

2.10.2 Fans Not Rotating Properly

Message Fan Module Failure Raised

Severity Minor

Explanation One or more of the fans in the fan module is not functioning properly. The fan could be obstructed by a foreign object or the fan may be faulty. If there are no obstructions then the fan module should be replaced.

Action Perform the following:

1. Verify that the environmental temperature requires a fan.
2. If the temperature is high enough to require a fan(s), reseat the module.
3. Replace the module if necessary.

Alarms The following components are affected:

	Component	Status	Alarm
•	FM4	Degraded	Minor / Major
•	FM7	Degraded	Minor / Major
•	FM8	Degraded	Minor / Major

Note: Alarm is Minor if less than half the fans are not rotating properly and Major if more than half the fans are not rotating properly.

2.10.3 Hardware Not Recognized

Message Fan Module Failure Raised

Severity Critical

Explanation A fan module has been inserted that the control module software does not recognize. The fans may or may not be operating. If the fans are not operating a shelf high temperature alarm may also be raised.

Action Perform the following:

1. Check the fan module.
2. Check the control module software and see whether it needs to updated to a newer release.

Alarms The following components are affected:

	Component	Status	Alarm
•	FAN8	Failed	Major
•	FM4	Failed	Major

2.10.4 High Temperature

Message Fan Module Failure Raised

Severity Major

Explanation There is a temperature sensor on the FM4, each CFC, and each PSU. (The FM4 has three.) Each sensor can report a High Temperature log (PSU001 for the PSU, CARD005 for the CFC, and FAN001 for the FM4).

Action Perform the following:

1. Input SHOW SYSTEM COOLING to see which components have had a temperature change and the status of the FM4.
2. Check the affected component and replace if necessary.
3. If multiple components are showing a temperature change, check the FM and replace if necessary.

Alarms The following components are affected:

	Component	Status	Alarm
•	FM4	Degraded	Major

2.10.5 No Communication

Message Fan Module Failure Raised

Severity Critical

Explanation The control module cannot communicate with the fan module. The fans may or may not be operating. If the fans are not operating a shelf high temperature alarm may also be raised.

Action Perform the following:

1. If the condition doesn't clear then the fan module is probably defective and should be replaced.

Alarms The following components are affected:

	Component	Status	Alarm
•	FAN8	Failed	Major
•	FM4	Failed	Major
•	FM7	Failed	Major

2.11 IGMP000 - mcHighWaterMarkPerCardExceeded

2.11.1 Not Applicable

Message MC count at High Threshold mark

Severity Major

Explanation The number of IGMP Reports that have been received on one Service Module is coming close to the provisioned slot's group limit (GRPLIMIT).

Action Perform the following:

1. Verify traffic engineering for this card.

Alarms The following components are affected:

Component Status Alarm

- None

2.12 IGMP001 - mcChannelLimitPerShelfExceeded

2.12.1 Not Applicable

Message Maximum Allowed Layer 2 MC Group limit reached

Severity Major

Explanation The number of concurrent multicast groups on the system has been reached. An IGMP Report is being dropped due to reaching the system's limit.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

Component Status Alarm

- None

2.13 IGMP002 - mcHighWaterMarkPerCardCleared

2.13.1 Not Applicable

Message MC count at High Threshold mark cleared

Severity Info

Explanation The IGMP group limit per card has dropped below the high water mark.

Action Perform the following:

- No action is required.

Alarms The following components are affected:

Component Status Alarm

- None

2.14 IGMP003 - mcGroupLimitPerMACExceeded

2.14.1 Not Applicable

Message MAC Addr <n> on slot <n> port <n> VID <n> tried to join <n> which would be more than 5 MC groups!

Severity Major

Explanation The subscriber device is requesting more MC groups (channels) than allowed.

Action Perform the following:

1. This could be an STB fault, so contact the subscriber.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.15 IGMP004 - mcMACLimitPerPortExceeded

2.15.1 Not Applicable

Message MAC Addr <n> on slot <n> port <n> VID <n> tried to join <n>, but 3 different MACs were already detected behind this port!

Severity Major

Explanation The maximum number of multicast devices per port has been exceeded.

Action Perform the following:

1. Contact the subscriber.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.16 IGMP005 - mcFirstRouterDetected

2.16.1 Not Applicable

Message Detected the First router on VID, IGMP report/leaves will NOW be accepted on this VID!

Severity Info

Explanation The first MC router has been detected on this VLAN, IGMP Snooping will now start processing Reports and Leaves.

Action Perform the following:

1. No action is required.

2.17 IGMP006 - mcNewRouterDetected

2.17.1 Not Applicable

Message Detected a router on VID <n> on slot <n> port <n>

Severity Info

Explanation A MC router has been detected. IGMP Reports and Leaves will now be forwarded to this MC router

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.18 IGMP007 - mcLastRouterAgedOut

2.18.1 Not Applicable

Message The Last MC Router had aged out on VID <n>, no IGMP report/leaves will be accepted on this VID!

Severity Info

Explanation The system is not receiving any router messages and has therefore timed out the last MC router on this VLAN. No IGMP Reports or Leaves will be processed for this VLAN.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.19 IGMP008 - mcRouterAgedOut

2.19.1 Not Applicable

Message A MC Router has aged out on VID on slot <n> port <n>

Severity Info

Explanation The system is not receiving any router messages and has therefore timed out a MC router on this VLAN.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.20 IGMP009 - (no Trap Message)

2.20.1 Not Applicable

Message IGMP Report Discarded due to Reserved Multicast MAC Address

Severity Info

Explanation The IGMP code validates the requested multicast IP address to insure that it is not within the reserved multicast IP address range (224.0.0.0 - 224.0.0.255). This range of multicast IP addresses are used for protocols only and are not controlled with IGMP (for example, OSPF, PIM, IGMP, etc.)

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.21 IGMP010 - (no Trap Message)

2.21.1 Not Applicable

Message IGMP Leave Discarded due to Reserved Multicast MAC Address

Severity Info

Explanation The IGMP code validates the requested multicast IP address to insure that it is not within the reserved multicast IP address range (224.0.0.0 - 224.0.0.255). This range of multicast IP addresses are used for protocols only and are not controlled with IGMP (for example, OSPF, PIM, IGMP, etc.)

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

	Component	Status	Alarm
•	None		

2.22 INTF003 - (no Trap Message)

2.22.1 Classifier Configuration Failed

Message `Interface Degradation Set`

Severity `Info`

Explanation `The reported interface has rejected the provisioned classifier configuration for an unspecified reason. CLASSIFIER and/or ACCESSLIST functionality may not behave correctly.`

Action `Perform the following:`

1. Verify classifier provisioning.
2. Disable and enable the interface.
3. Disable and enable the card.
4. If the problem still exists, contact Allied Telesis Support.

Alarms `The following components are affected:`

	Component	Status	Alarm
•	ATMBOND	Degraded	Info
•	ONU	Degraded	Info
•	PPP	Degraded	Minor

2.22.2 Classifier Configuration Not Supported

Message `Interface Degradation Set`

Severity `Info`

Explanation `The reported interface is not capable of supporting the provisioned classifier configuration. This may be due to the reported card running an older software revision. CLASSIFIER and/or ACCESSLIST functionality may not behave correctly.`

Action `Perform the following:`

1. Verify software release running in the associated card.
2. Verify classifier provisioning.
3. Disable and enable the interface.
4. Disable and enable the card.
5. If the problem still exists, contact Allied Telesis Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	ATMBOND	Degraded	Info
•	MLPPP	Degraded	Minor
•	ONU	Degraded	Info
•	PPP	Degraded	Minor

2.22.3 Classifier Resources Exceeded

Message Interface Degradation Set

Severity Info

Explanation The reported interface has exceeded the maximum resources available for classifier configuration. CLASSIFIER and/or ACCESSLIST functionality may not behave correctly.

Action Perform the following:

1. Verify classifier provisioning.
2. Disable and enable the interface.
3. Disable and enable the card.
4. If the problem still exists, contact Allied Telesis Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	ATMBOND	Degraded	Info
•	MLPPP	Degraded	Minor
•	ONU	Degraded	Info
•	PPP	Degraded	Minor

2.23 IPIF001 - (To Be Supplied)

2.23.1 IP Interface Configuration Failed

Message To Be Supplied

Severity Info

Explanation IP interface configuration failed. This alarm is more likely on the INBAND interface than the MGMT interface, since more configuration is required (CFC and line card for INBAND, as opposed to just CFC for MGMT). Note that internal classifiers are used on the line cards hosting the inband VLANs for traffic extraction to the CFC.

Action Perform the following:

1. Disable/enable the failed interface to make the system reattempt the configuration.
2. If failure persists contact Allied Telesis support.

Alarms The following components are affected:

	Component	Status	Alarm
•	IP Interface	Failed	Minor

2.24 LOG005 - atnMediaLogStreamError

2.24.1 I/O error writing to compact flash

Message Failed to write management logs to storage media

Severity Major

Explanation The user has configured log streaming to a compact flash card, but streaming can no longer occur because the card is full or is no longer present.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	None		

2.24.2 Compact flash unit deactivated

Message Failed to write management logs to storage media

Severity Major

Explanation The user has deactivated this CFLASH unit. It won't be available for use again until it is activated.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	None		

2.24.3 Compact flash media not present

Message Failed to write management logs to storage media

Severity Major

Explanation The user has configured log streaming to a compact flash card, but streaming can no longer occur because the card is no longer present. The CFLASH card has been extracted from the unit.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.25 LOG006 - Not Applicable

2.25.1 Not Applicable

Message Failed to write management logs to storage media

Severity Info

Explanation This log indicates that en existing alarm condition, a failure to write management logs to storage media, has been cleared. This usually means that a CFLASH unit that was under an alarm condition is now available for use.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.26 PORT003 - Linkdown

2.26.1 BFD Detected Miswiring

Message Port Fault Set

Severity Info

Explanation For Bi-Directional Forwarding Detection (BFD), produced when an interface is receiving an incorrect discriminator, and so the interface is not receiving BFD frames from the same pair it is sending them to.

Action Perform the following:

1. Check the wiring.

Alarms The following components are affected:

Component	Status	Alarm
• FE Port	Failed	Info
• GE Port	Failed	Major
• XE Port	Failed	Major

2.26.2 BFD Session Failed

Message Port Fault Set

Severity Info

Explanation For Bi-Directional Forwarding Detection (BFD), produced when an interface has not received BFD packets within the configured interval timer times the detection multiplier. The connection may be lost even though there is no link (LOS) failure.

Action Perform the following:

1. Check the configuration.

Alarms The following components are affected:

Component	Status	Alarm
• FE Port	Failed	Info
• GE Port	Failed	Major
• XE Port	Failed	Major

2.26.3 Config Failed

Message Port Fault Set

Severity Info

Explanation The port failed to configure. This could be due to high traffic through the card, a problem with provisioning associated with the port.

Action Perform the following:

1. Verify traffic capacity.
2. Verify load preferences.
3. Verify provisioning.

Alarms The following components are affected:

Component	Status	Alarm

• ADSL Port	Failed	Info
• SS1 Port	Failed	Major
• E1 Port	Failed	Major
• EPON Port	Failed	Major
• FE Port	Failed	Major
• FX Port	Failed	Major
• GE Port	Failed	Major
• POTS Port	Failed	Info
• SHDSL Port	Failed	Info
• XE Port	Failed	Major

2.26.4 Disable Failed

Message `Port Fault Set`

Severity `Minor`

Explanation `The port failed to respond to a disable request. It could be due to high traffic through the card, a problem with provisioning associated with the port.`

Action `Perform the following:`

1. `Verify traffic capacity.`
2. `Verify load preferences.`
3. `Verify provisioning.`

Alarms `The following components are affected:`

Component	Status	Alarm
• ADSL Port	Failed	N/A
• DS1 Port	Failed	N/A
• E1 Port	Failed	N/A
• EPON Port	Failed	N/A
• FE Port	Failed	None
• FX Port	Failed	None
• GE Port	Offline	None
• POTS Port	Failed	None
• SHDSL Port	Failed	N/A
• XE Port	Offline	None

2.26.5 Enable Failed

Message Port Fault Set

Severity Info

Explanation The port failed to respond to an enable request. It could be due to high traffic through the card, or a problem with provisioning associated with the port.

Action Perform the following:

1. Verify traffic capacity.
2. Verify load preferences.
3. Verify provisioning.

Alarms The following components are affected:

Component	Status	Alarm
• ADSL Port	Failed	Info
• DS1 Port	Failed	Major
• E1 Port	Failed	Major
• EPON Port	Failed	Major
• FE Port	Failed	Major
• FX Port	Failed	Major
• GE Port	Failed	Major
• POTS Port	Failed	Info
• SHDSL Port	Failed	Info
• XE Port	Failed	Major

2.26.6 Loss of Frame (LOF)

Message Port Fault Set

Severity Major

Explanation The port has lost the framing source from the far end equipment

Action Perform the following:

1. Verify framing source.
2. Verify far-end equipment.
3. Disable/enable the port.

Alarms The following components are affected:

Component	Status	Alarm

• ADSL Port	Degraded	Info
• DS1 Port	Failed	Major
• E1 Port	Failed	Major
• GE Card	Failed	Major
• SHDSL Port	Failed	Info
• XE Port	Failed	Major

2.26.7 Loss of Link (LOL)

Message `Port Fault Set`

Severity `Info`

Explanation `Essentially the same as LOS. The only difference between the two is that LOS is preceded by a "last gasp" message where LOL does not. The connections or far-end equipment could be at fault.`

Action `Perform the following:`

1. Verify connections.
2. Verify far-end equipment.
3. Disable/enable port.

Alarms `The following components are affected:`

Component	Status	Alarm
• ADSL Port	Failed	Info
• FE Port	Failed	Info
• FX Port	Failed	Info
• GE Port	Failed	Major
• SHDSL Port	Failed	Info
• XE Port	Failed	Major

2.26.8 Loss of Signal (LOS)

Message `Port Fault Set`

Severity `Major`

Explanation `The port is no longer receiving a signal from the far end equipment. The connections or far-end equipment could be at fault.`

Action `Perform the following:`

1. Verify sync source.

2. Verify far-end equipment.
3. Disable/enable port.

Alarms The following components are affected:

Component	Status	Alarm
• ADSL Port	Failed	Info
• DS1 Port	Failed	Major
• E1 Port	Failed	Major
• EPON Port	Failed	Major
• GE Port	Failed	Major
• SHDSL Port	Failed	Info
• XE Port	Failed	Major

2.26.9 Loss of Sync (LOSY)

Message Port Fault Set

Severity Major

Explanation The port has lost the sync source from the far end equipment.

Action Perform the following:

1. Verify sync source.
2. Verify far-end equipment.
3. Disable/enable port.

Alarms The following components are affected:

Component	Status	Alarm
• GE Port	Failed	Major
• XE Port	Failed	Major

2.26.10 Remote BFD Session Failed

Message Port Fault Set

Severity Info

Explanation For Bi-Directional Forwarding Detection (BFD), produced when the remote interface is reporting that its BFD State is down. The connection may be lost even though there is no link (LOS) failure.

Action Perform the following:

1. Check the wiring/connections with the remote interface.

Alarms The following components are affected:

	Component	Status	Alarm
•	FE Port	Failed	Info
•	GE Port	Failed	Major
•	XE Port	Failed	Major

2.26.11 Reset Failed

Message Port Fault Set

Severity Info

Explanation Port failed to respond to reset request. This could be due to high traffic through the card, or a problem with provisioning associated with the port.

Action Perform the following:

1.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL Port	Failed	Info
•	CFC200	Failed	Major
•	GE Port	Failed	Major
•	SHDSL Port	Failed	Info
•	XE Port	Failed	Major

2.26.12 SFP Not Present

Message Port Fault Set

Severity Info

Explanation No SFP is physically present in the GE port.

Action Perform the following:

1. Insert the correct SFP into the port.

Alarms The following components are affected:

	Component	Status	Alarm
•	GE24SFP	Failed	Major

2.26.13 Unexpected BPDU Received

Message Port Fault Set

Severity Info

Explanation This failing alarm is raised when a BPDU is received on an interface that has BPDU cop feature enabled. The BPDU cop feature protects the system from network loops and other threats where the symptom is reception of an unexpected BPDU.

Action Perform the following:

1. Disable/enable the interface.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL Port	AutoDisabled	Info
•	FE Port	AutoDisabled	Info
•	FX Port	AutoDisabled	Info
•	GE Port	AutoDisabled	Major
•	SHDSL Port	AutoDisabled	Info
•	XE Port	AutoDisabled	Major

2.26.14 XFP Not Present

Message Port Fault Set

Severity Info

Explanation No XFP is physically present in the XE port.

Action Perform the following:

1. Insert the correct XFP into the port.

Alarms The following components are affected:

	Component	Status	Alarm
•	XE4	Failed	Major

2.27 PORT005 - atnPortDefectRaised

2.27.1 Classifier Configuration Failed

Message Port Degradation Set

Severity Minor

Explanation The reported card/port has rejected the provisioned classifier configuration for an unspecified reason. CLASSIFIER and/or ACCESSLIST functionality may not behave correctly.

Action Perform the following:

1. Verify classifier provisioning.
2. Disable and enable the port.
3. Disable and enable the card.
4. If the problem still exists, contact Allied Telesis Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL Port	Degraded	Info
•	FE Port	Degraded	Minor
•	FX Port	Degraded	Minor
•	GE Port	Degraded	Minor
•	IP Interface	Degraded	Minor
•	MLPPP	Degraded	Minor
•	SHDSL Port	Degraded	Minor
•	XE Port	Degraded	Minor

2.27.2 Classifier Configuration Not Supported

Message Port Degradation Set

Severity Minor

Explanation The reported card/port is not capable of supporting the provisioned classifier configuration. This may be due to the reported card running an older software revision. CLASSIFIER and/or ACCESSLIST functionality may not behave correctly.

Action Perform the following:

1. Verify software release running in the associated card.
2. Verify classifier provisioning.
3. Disable and enable the port.
4. Disable and enable the card.
5. If the problem still exists, contact Allied Telesis Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL Port	Degraded	Minor
•	FE Port	Degraded	Info
•	FX Port	Degraded	Minor

• GE Port	Degraded	Minor
• IP Interface	Degraded	Minor
• SHDSL Port	Degraded	Minor
• XE Port	Degraded	Minor

2.27.3 Classifier Resources Exceeded

Message `Port Degradation Set`

Severity `Minor`

Explanation `The reported card/port has exceeded the maximum resources available for classifier configuration. CLASSIFIER and/or ACCESSLIST functionality may not behave correctly.`

Action `Perform the following:`

1. Verify classifier provisioning.
2. Disable and enable the port.
3. Disable and enable the card.
4. If the problem still exists, contact Allied Telesis Support.

Alarms `The following components are affected:`

Component	Status	Alarm
• ADSL Port	Degraded	Minor
• FE Port	Degraded	Info
• FX Port	Degraded	Minor
• GE Port	Degraded	Minor
• IP Interface	Degraded	Minor
• SHDSL Port	Degraded	Minor
• XE Port	Degraded	Minor

2.28 RMON001 - risingAlarm

2.28.1 Not Applicable

Message `Rising Alarm. Index:`

Severity `Minor`

Explanation `A rising alarm is generated when a Remote Monitoring (RMON) statistic crosses over a user provisioned threshold over a specified period of time. The message contains the index of the ethernet interface affected, the specific statistic involved, the type of`

sample used (Change vs. Absolute), the current value of the statistic, and the provisioned threshold. The message is an alert to a user to indicate the presence or potential for problems on a specific interface. Since the threshold values are user defined, the message is considered informational.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.29 RMON002 - fallingAlarm

2.29.1 Not Applicable

Message Falling Alarm. Index:

Severity Info

Explanation A falling alarm is generated when a Remote Monitoring (RMON) statistic crosses below a user provisioned threshold during a specified period of time. The message contains the index of the ethernet interface affected, the specific statistic involved, the type of sample used (Change vs. Absolute), the current value of the statistic, and the provisioned threshold. The message is an alert to a user to indicate the presence or potential for problems on a specific interface. Since the threshold values are user defined, the message is considered informational.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.30 SHLF001 - atnShelfFaultRaised

2.30.1 Port Outage Threshold

Message Port Fault Set

Severity Variable

Explanation The level of alarm depends on the number of downstream interfaces affected. (More than 128=Critical, 25 to 128=Major, Less than 24=Minor)

Action Perform the following:

1. Restore the failed uplinks.
2. Restore any failed service modules.

Alarms The following components are affected:

	Component	Status	Alarm
•	Shelf	N/A	Critical
•	Shelf	N/A	Major
•	Shelf	N/A	Minor

Note: More than 128 downstream ports are impacted by card faults, and/or there is no uplink available.

2.30.2 VLAN has no NETWORK facing interface

Message Shelf Failure Raised\nReason:

Severity Major

Explanation This alarm is raised when a vlan is in UFO mode and there is no upstream interface for whatever reason: no upstream interface is configured, the upstream interface is down, EPSR/STP/UCP could not find an upstream to use. The alarm will be cleared when: the vlan is changed to STD mode, or an upstream interface is found (configured, link comes up, or EPSR/STP/UCP finds an upstream to use).

Action Perform the following:

1. Change the VLAN to non-UFO or ensure (configure) an upstream link.

Alarms The following components are affected:

	Component	Status	Alarm
•	Shelf	N/A	Major

2.31 SYS004 - atnCardDefectRaised

2.31.1 Database Audit Failure

Message Database Audit Failure. A restart may be necessary

Severity Minor

Explanation A routine audit has discovered a discrepancy between the data running in RAM and the data stored in the system database. On a duplex system, if the failure is on the inactive CFC only, then the system automatically restarts the inactive CFC to cause a resync to fix the problem. Whether a simplex or duplex system, if the failure is on the active CFC then manual action is required, and any configuration changes made by users are not saved to the system database.

Action Perform the following:

1. Restart the CFC
2. If necessary, go to the last known backup.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC12	Degraded	Minor
•	CFC200	Degraded	Minor
•	CFC200	Failed	Minor
•	CFC24	Degraded	Minor
•	CFC24	Failed	Minor
•	CFC4	Degraded	Minor
•	CFC6	Degraded	Minor
•	CFC6	Failed	Minor

Note: For an active CFC, the status is Degraded, since there is no backup CFC.

2.31.2 Database Transaction Failure

Message Database Transaction Failure

Severity Major

Explanation While this alarm is present any persistent configuration data that is entered may not be stored in the persistent database. (**CAUTION**: While this alarm is present any persistent configuration data that is entered may not be stored in the persistent database.)

Action Perform the following:

1. All management logs, error, and crash logs should be collected and the database restored (RESTORE DATABASE)
2. Recover with a database restoration using the RESTORE DATABASE command.
3. Contact Allied Telesis Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC12	Degraded	Major
•	CFC200	Degraded	Major
•	CFC200	Failed	Major
•	CFC24	Degraded	Major
•	CFC24	Failed	Minor
•	CFC4	Degraded	Major
•	CFC6	Degraded	Major
•	CFC6	Failed	Minor

Note: For an active CFC, the status is Degraded, since there is no backup CFC.

2.31.3 Death of non-critical task

Message `Death of non-critical task`

Severity `Major`

Explanation `A software task in the system has failed, but the task is deemed non-critical in terms of service impact, thus no automatic reboot is necessary. A manually initiated reboot may be necessary to correct the alarm if it doesn't clear on its own.`

Action `Perform the following:`

1. Capture ALL logs.
2. Contact Allied Telesis Support.

Alarms `The following components are affected:`

	Component	Status	Alarm
•	CFC12	Degraded	Major
•	CFC200	Degraded	Minor
•	CFC24	Degraded	Major
•	CFC24	Degraded	Minor
•	CFC4	Degraded	Major
•	CFC6	Degraded	Major
•	CFC6	Degraded	Minor

Note: When this occurs with an active CFC200, a swap is possible.

2.31.4 Flash Write Failure

Message `To Be Supplied`

Severity Major

Explanation A failure to write to the flash memory has occurred while trying to write to the database.

Action Perform the following:

1. Most likely this indicates a problem with the flash part on the card, the user probably needs to replace the card.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC200	Online	Major
•	CFC24	Online	Major
•	CFC56	Online	Major

2.32 SYS009 - atnShelfFaultRaised

2.32.1 Cannot Read MAC Address

Message System: Raised Can Not Read MAC Address

Severity Major

Explanation The MAC card is defective.

Action Perform the following:

1. Contact Allied Telesis Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	Shelf	N/A	Major

2.33 TRAP003 - coldStartTrap

2.33.1 Not Applicable

Message Cold Start Trap

Severity Major

Explanation Cold start trap for device initialization. No management log is generated.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

Component	Status	Alarm

- None

2.34 TRAP004 - warmStart

2.34.1 Not Applicable

Message Warm Start Trap

Severity Major

Explanation Warm start trap for an activity change. No management log generated.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

Component	Status	Alarm

- None

2.35 TRAP009 - entConfigChangeTrap

2.35.1 Not Applicable

Message Entity config change trap

Severity Warning

Explanation A provisioning change on the shelf was performed. The change may have occurred to the shelf, a card in the shelf, or a physical port.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

Component	Status	Alarm

- None

4. iMAP Logs with Traps

1 Overview

This section is organized as follows.

1.1 Listing of Logs and Traps

This is a table that lists the log category / trap text that is the entry point for log descriptions. Each entry is a live link to the section that includes all of the reason codes.

1.2 Log and Trap Listing by Reason Code

This includes an overview of the log category / trap text and then a description for each Reason Code. For each Reason Code there are the following attributes:

- Message
- Severity
- Explanation
- Action
- Alarms - This is a list of components that can be affected, and includes any special notes because of the component type.

2 Listing of Logs and Traps

The following table lists the logs and trap text that apply to the iMAP product only.

TABLE 4-1 Logs and Traps for iMAP

Log and Trap Text	Reason Code (or Message)
ADSL021- adslAtucPerfLofsThreshTrap	Not Applicable
ADSL022 - adslAturPerfLossThreshTrap	Not Applicable
ADSL024 - adslAtucPerfLprsThreshTrap	Not Applicable
ADSL025 - adslAtucPerfESsThreshTrap	Not Applicable
ADSL026 - adslAturPerfLofsThreshTrap	Not Applicable
ADSL028 - adslAturPerfLprsThreshTrap	Not Applicable
ADSL029 - adslAturPerfESsThreshTrap	Not Applicable
ADSL030 - adslAtucPerfSesLThreshTrap	Not Applicable
ADSL031 - adslAtucPerfUasLThreshTrap	To Be Supplied
ADSL032 - adslAturPerfSesLThreshTrap	Not Applicable
ADSL033 - adslAturPerfUasLThreshTrap	Not Applicable
ADSL034 - adslAtucFailedFastRThreshTrap	Not Applicable
CARD001 - entConfigChangeTrap	Slot Provisioning Mismatch

TABLE 4-1 **Logs and Traps for iMAP**

Log and Trap Text	Reason Code (or Message)
CARD005 - atnCardDefectRaised	DSP Core Fault Power 18 Failed Power 25 Adj. Failed Power A Failed Power B Failed Power Fuse Failed SB 2.5v Power Failed SB CPU 2.5v Power Failed SB 2.5v ANALOG Power Failed SB 2.5v DIGITAL Power Failed Ring Generator Overload Ring Generator Failure Lost Communication with Call Server DSP Failure Configuration Incomplete Hardware Unsupported Incompatible with Active Internal Oscillator Failure

TABLE 4-1 **Logs and Traps for iMAP**

Log and Trap Text	Reason Code (or Message)
CARD005 - atnCardDefectRaised - Cont'd	Unable to Load DNS Server Timed Out ARP Resolution Failed DNS resolution failed CFlash Failed AC Power A Failed AC Power B Failed AC Power A Fan Failed AC Power B Fan Failed 1.2v Power Failed Duplicate IP Address IP buffer pool exhausted Power Input Incompatibility Inconsistent Flooding Card Disable Failed Protocol Mismatch Incompatible Load Unsupported Hardware
CARD023 - atnCardDefectRaised	Sync Card Not Detected Loss of Primary Reference Loss of Secondary Reference Loss of Holdover Sync Card Clock Error
CARD046 - ATNCARDFDBMGMTOVER-FLOW	Not Applicable
CUC001 - atnCUCFaultRaised	Not Present Power Supply Failure No Communication
FAN001 - atnCUCFaultRaised	Hardware Not Recognized
FAN001 - atnFanFaultRaised	Fan Module Power Supply Failure

TABLE 4-1 **Logs and Traps for iMAP**

Log and Trap Text	Reason Code (or Message)
INTF001 - Linkdown	All parents non-administratively down Config Failed Echo Request Timeout Loopback Detected Negotiation Failed Peer Disabled ONU Not Discovered Remote Tranmsit Failed Loading Firmware Waiting to Load Firmware Not Applicable All Links Failed Unexpected BPDU Received Report Timeout Links Not Discovered All ASM Links Down All Parent Interfaces Down Loss of Signal (LOS) Alarm Indication Signal SFP Type Mismatch SFP Not Present Receive Loss of Lock Remote Defect Indication
INTF003 - Unknown	Bandwidth Degraded

TABLE 4-1 **Logs and Traps for iMAP**

Log and Trap Text	Reason Code (or Message)
INTF003 - atnInterfaceDefectRaised	Keep Alive Timeout Remote Loss of Signal (UNI) Remote Gate Timeout Remote Keep Alive Timeout Mismatched ONU Type Unsupported ONU Type No Response from BRAS Negotiation Failed Echo Request Timeout Below Min Downstream Aggregate Rate Below Min Upstream Aggregate Rate Downstream Differential Rate Exceeded Some ASM Links Down Some Parent Interfaces Down Status Attribute Upstream Differential Rate Exceeded Excessive Zeroes Bipolar Violation Far-End SEF AIS Out of Frame
INTF003 - Linkdown	Loss of Frame (LOF)
PMON001 - atnDs1CurrentLCVThreshTrap	Not Applicable
PMON002 - atnDs1CurrentLESThreshTrap	Not Applicable
PMON003 - atnDs1CurrentLOSThreshTrap	Not Applicable
PMON004 - atnDs1CurrentSESThreshTrap	Not Applicable
PMON005 - atnDs1DayUASThreshTrap	Not Applicable

TABLE 4-1 **Logs and Traps for iMAP**

Log and Trap Text	Reason Code (or Message)
PORT003 - Linkdown	CAS Thermal Shutdown SLIC Thermal Shutdown AC Fault DC Fault PCM Clock Failure Battery Failure No Peer Present (NPP) Loopback Failed Timing Reference Failed Link Quality Failed Loss of RTP Receive Stream Loss of RTP Transmit Stream Receiving AIS Receiving RAI Transmit Failed No Links Discovered Loading Firmware Interface Internal Failure Registration Failed DS3 Out of Service
PORT005 - HDSL2SHDSLPERFLOSWSTHRESH	Loss Of Sync Word
PORT005 - atnPortDefectRaised	Loss Of Signal Quality (LOSQE) Loss of Power - Modem Off (LPR) Transmit Degraded Downstream Bandwidth Resources Exceeded Bandwidth Priority Category Resources Exceeded Link Threshold Exceeded
PORT005 - Linkdown	Loss of Cell Delineation

TABLE 4-1 **Logs and Traps for iMAP**

Log and Trap Text	Reason Code (or Message)
PORT005 - Not applicable	Timing Reference Degraded
PORT005 - atnPortDefectCleared	Upstream Bandwidth Resources Exceeded
PORT013 - Not applicable	High priority queue overflow
PORT013 - To Be Supplied	Port AIS Received
PORT017 - Not applicable	Not Applicable Not Applicable
PSPN003 - atnPSpanDefectRaised	ARP Resolution Failed DNS resolution failed DNS Server Timed Out PSPAN Configuration Failed PSPAN does not have a connection PSPAN Egress Path Failed PSPAN Ingress Path Failed PSPAN LOPS PSPAN Remote LOPS PSPAN Timing Reference Degraded PSPAN Timing Reference failed
SHLF001 - atnShelfFaultRaised	Can Not Read Temperature Sensors High Shelf Temperature High Temperature
SHLF008 - atnDryContactRaised	Unknown
SHLF009 - atnDryContactCleared	Unknown Unknown
SYS004 - atnMediaLogStreamError	CFlash Failed
SYS009 - atnShelfFaultRaised	Packet Overflow
XDSL001 - HDSL2SHDSLPERFLOSWSTHRESH	Not Applicable

TABLE 4-1 **Logs and Traps for iMAP**

Log and Trap Text	Reason Code (or Message)
XDSL002 - HDSL2SHDSLPERFCRCANOMALIESTHRESH	Not Applicable
XDSL003 - HDSL2SHDSLPERFESTHRESH	Not Applicable
XDSL004 - HDSL2SHDSLPERFSESTHRESH	Not Applicable
XDSL005 - HDSL2SHDSLPERFUASTHRESH	Not Applicable
XDSL006 - HDSL2SHDSLPERFLOSWSTHRESH	Not Applicable
XDSL007 - HDSL2SHDSLPERFCRCANOMALIESTHRESH	Not Applicable Not Applicable
XDSL008 - HDSL2SHDSLPERFESTHRESH	Not Applicable
XDSL009 - HDSL2SHDSLPERFSESTHRESH	Not Applicable
XDSL010 - HDSL2SHDSLPERFUASTHRESH	Not Applicable
XDSL018 - xdslPortQualityRetrain	Retrain: Line Quality
XDSL019 - xdslPortStuckHandShakeRetrain	Retrain: Handshake Stuck
XDSL020 - xdslPortMinDownRateRetrain	Retrain: Minimum Downstream Rate
XDSL021 - xdsllossofmarginretrain	Retrain: SNR Margin Threshold

2.1 ADSL021- adslAtucPerfLofsThreshTrap

2.1.1 Not Applicable

```
Message      Atuc (Near End) Loss of Framing TCA on port
Severity     Minor
```

Explanation The interface is carrying a signal, but the ADSL card is unable to frame against the signal. As a result, all packets are being tossed.

Action Perform the following:

1. Verify that the provisioning characteristics of the ADSL port match those of the device to which it is attached.
2. If there are any differences, correct them.
3. If there are no differences, attempt disabling and then re-enabling the port to see if the problem persists.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.2 ADSL022 - adslAturPerfLossThreshTrap

2.2.1 Not Applicable

Message Atur (Far End) Loss of Signal TCA on port

Severity Minor

Explanation The interface is no longer receiving a signal from far-end equipment. The number of seconds the LOS defect has existed exceeds the provisioned threshold for the current 15-minute period.

Action Perform the following:

1. Check the far-end equipment to make sure that it is still in-service.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.3 ADSL024 - adslAtucPerfLprsThreshTrap

2.3.1 Not Applicable

Message Atuc (Near End) Loss of Power TCA on port

Severity Minor

Explanation Normally means the far end equipment has been powered-down. The number of seconds the LPR defect has existed exceeds the provisioned threshold for the current 15-minute period.

Action Perform the following:

1. Check the far end equipment.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.4 ADSL025 - adslAtucPerfESsThreshTrap

2.4.1 Not Applicable

Message Atuc (Near End) Errored Seconds TCA on port

Severity Minor

Explanation The number of errored seconds has existed exceeds the provisioned threshold for the current 15-minute period.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.5 ADSL026 - adslAturPerfLofsThreshTrap

2.5.1 Not Applicable

Message Atur (Far End) Loss of Framing TCA on port

Severity Minor

Explanation The ATU-R Loss of Framing (LOF) Threshold Crossing Alert (TCA) trap provides an alert that a given ADSL interface has crossed its user provisioned LOF threshold during a given 15-minute interval. Once generated during a 15-minute interval, the alert is not generated again until the threshold is verified again in the next 15-minute interval. The alert indicates a given interface has experienced a cumulative LOF condition in excess of what is desired in a 15-minute interval. Typically, the alert is generated every fifteen minutes until the problem is corrected or until a user changes the threshold value.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component Status Alarm

- None

2.6 ADSL028 - adslAturPerfLprsThreshTrap

2.6.1 Not Applicable

Message Atur (Far End) Loss of Power TCA on port

Severity Minor

Explanation The ATU-R Loss of Power (LPRS) Threshold Crossing Alert (TCA) trap provides an alert that a given ADSL interface has crossed its user provisioned LPRS threshold during a given 15-minute interval. Once generated during a 15-minute interval, the alert is not generated again until the threshold is crossed again in the next 15-minute interval. The alert indicates that a given interface has experienced a cumulative loss of power condition for a number of seconds in excess of what is desired in a 15-minute interval. Typically, the alert is generated every fifteen minutes until the problem is corrected or until a user changes the threshold value.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component Status Alarm

- None

2.7 ADSL029 - adslAturPerfESsThreshTrap

2.7.1 Not Applicable

Message Atur (Far End) Errored Seconds TCA on port

Severity Minor

Explanation The ATU-R Errored Seconds (ES) Threshold Crossing Alert (TCA) trap provides an alert that a given ADSL interface has crossed its user provisioned ES threshold during a given 15-minute interval. Once generated during a 15-minute interval, the alert is not generated again until the threshold is crossed again in the next 15-minute interval. The alert indicates that a given interface has experienced a cumulative ES condition in excess of what is desired in a 15-minute interval. Typically, the alert is generated every fifteen minutes until the problem is corrected or until a user changes the threshold value.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.8 ADSL030 - adslAtucPerfSesLThreshTrap

2.8.1 Not Applicable

Message Atuc (Near End) Severely Errored Seconds TCA on port

Severity Minor

Explanation The ATU-C Severely Errored Seconds (SES) Threshold Crossing Alert (TCA) trap provides an alert that a given ADSL interface has crossed its user provisioned SES threshold during a given 15-minute interval. Once generated during a 15-minute interval, the alert is not generated again until the threshold is crossed again in the next 15-minute interval. The alert indicates that a given interface has experienced a cumulative SES condition in excess of what is desired in a 15-minute interval. Typically, the alert is generated every fifteen minutes until the problem is corrected or until a user changes the threshold value.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.9 ADSL031 - adslAtucPerfUasLThreshTrap

2.9.1 To Be Supplied

Message Atuc (Near End) Unavailable Seconds TCA on port

Severity Info

Explanation The ATU-C Unavailable Seconds (UAS) Threshold Crossing Alert (TCA) trap provides an alert that a given ADSL interface has crossed its user provisioned UAS threshold during a given 15-minute interval. Once generated during a 15-minute interval, the alert is not generated again until the threshold is crossed again in the next 15-

minute interval. The alert indicates that a given interface has experienced a cumulative unavailable condition in excess of what is desired in a 15-minute interval. Unavailable seconds occur in response to the failure of an interface. It is possible to see this alert in conjunction with a LOS TCA. Typically, the alert is generated every fifteen minutes until the problem is corrected or until a user changes the threshold value.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.10 ADSL032 - adslAturPerfSesLThreshTrap

2.10.1 Not Applicable

Message Atur (Far End) Severely Errored Seconds TCA on port

Severity Minor

Explanation The ATU-R Severely Errored Seconds (SES) Threshold Crossing Alert (TCA) trap provides an alert that a given ADSL interface has crossed its user provisioned SES threshold during a given 15-minute interval. Once generated during a 15-minute interval, the alert is not generated again until the threshold is crossed again in the next 15-minute interval. The alert indicates that a given interface has experienced a cumulative SES condition in excess of what is desired in a 15-minute interval. Typically, the alert is generated every fifteen minutes until the problem is corrected or until a user changes the threshold value.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.11 ADSL033 - adslAturPerfUasLThreshTrap

2.11.1 Not Applicable

Message Atur (Far End) Unavailable Seconds TCA on port

Severity Info

Explanation The IGMP group limit per card has dropped below the high water mark.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.12 ADSL034 - adslAtucFailedFastRThreshTrap

2.12.1 Not Applicable

Message Atuc (Near End) Failed Fast Retrains TCA on port

Severity Info

Explanation The ATU-C Failed Fast Retrains Threshold Crossing Alert (TCA) trap provides an alert that a given ADSL interface has crossed its user provisioned fast retrain limit during a given 15-minute interval. Once generated during a 15-minute interval, the alert is not generated again until the threshold is crossed again in the next 15-minute interval. The alert indicates that a given interface has experienced a cumulative fast retrain failure condition in excess of what is desired in a 15-minute interval. Typically, the alert is generated every fifteen minutes until the problem is corrected or until a user changes the threshold value.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.13 CARD001 - entConfigChangeTrap

2.13.1 Slot Provisioning Mismatch

Message To Be Supplied

Severity Minor

Explanation A possible mis-provision double wide cards. The slots pre-provisioned for the card do not match the physical card presence. The

ADSL48 card is provisioned in 2 slots and physically occupies 2 slots. The ADSL24SA card is provisioned in 1 slot but physically occupies 2 slots. With either card its possible to insert the card where it mismatches the pre-provisioning. For example, Slot 1 pre-provisioned with FE10, slot 2-3 pre-provisioned with ADSL48. Plugging in the ADSL48 in slots 1-2 causes slot provisioning mismatch alarm in slot 1.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• ADSL	Not Installed	Minor
• CES8	Not Installed	Minor
• CFC24	Not Installed	Minor
• CFC56	Not Installed	Minor
• EPON2	Not Installed	Major
• FE10	Not Installed	Minor
• FX10	Not Installed	Minor
• GE	Not Installed	Major
• NTE8	Not Installed	Major
• POTS24	Not Installed	Minor
• SHDSL24	Not Installed	Minor
• VDSL24	Not Installed	Minor
• XE	Not Installed	Major

2.14 CARD005 - atnCardDefectRaised

2.14.1 DSP Core Fault

Message Card Failure Raised

Severity Minor

Explanation The card has a defective signal processor that is affecting all or part of it's functionality.

Action Perform the following:

1. Replace the card

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL Card	Degraded	Minor
•	SHDSL24	Degraded	Minor

2.14.2 Power 18 Failed

Message `Card Failure Raised`

Severity `Critical`

Explanation `A problem has been detected with the 1.8v power output on the CFC switch board, affecting data packet processing. The CFC card is probably defective.`

Action `Perform the following:`

1. For simplex systems, replace the CFC card.
2. For duplex systems, swap activity, then replace the faulty card.
3. If the problem is still not resolved, contact Allied Telesis Technical Support.

Alarms `The following components are affected:`

	Component	Status	Alarm
•	CFC4	Degraded	Critical
•	CFC6	Degraded	Critical
•	CFC6	Failed	Minor

2.14.3 Power 25 Adj. Failed

Message `Card Failure Raised`

Severity `Critical`

Explanation `A problem has been detected with the 2.5v power output on the CFC switch board, affecting data packet processing. The CFC card is probably defective.`

Action `Perform the following:`

1. For simplex systems, replace the CFC card.
2. For duplex systems, swap activity, then replace the faulty card.
3. If the problem is still not resolved, contact Allied Telesis Technical Support

Alarms `The following components are affected:`

	Component	Status	Alarm
•	CFC4	Degraded	Critical
•	CFC6	Degraded	Critical

• CFC6	Failed	Minor

2.14.4 Power A Failed

Message `Card Failure Raised`

Severity `Minor`

Explanation `A shelf power failure on power feed A has been detected by the control module card in the specified slot. The problem could be due to the external power feed to the shelf, a defective PEM, or the control module itself may be defective.`

Action `Perform the following:`

1. In a duplex system, if alarm is on only one card, then replace the card.
2. Otherwise, verify power feed to shelf.
3. Replace PEM.
4. Replace CFC card.
5. If the problem is still not resolved, contact Allied Telesis Technical Support

Alarms `The following components are affected:`

	Component	Status	Alarm
•	CFC12	Degraded	Minor
•	CFC24	Degraded	Minor
•	CFC24	Degraded	Minor
•	CFC4	Degraded	Minor
•	CFC6	Degraded	Minor
•	CFC6	Degraded	Minor

2.14.5 Power B Failed

Message `Card Failure Raised`

Severity `Minor`

Explanation `A shelf power failure on power feed A has been detected by the control module card in the specified slot. The problem could be due to the external power feed to the shelf, a defective PEM, or the control module itself may be defective.`

Action `Perform the following:`

1. In a duplex system, if alarm is on only one card, then replace the card.
2. Otherwise, verify power feed to shelf.
3. Replace PEM.

4. Replace CFC card.
5. If the problem is still not resolved, contact Allied Telesis Technical Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC12	Degraded	Minor
•	CFC24	Degraded	Minor
•	CFC24	Degraded	Minor
•	CFC4	Degraded	Minor
•	CFC6	Degraded	Minor
•	CFC6	Degraded	Minor

2.14.6 Power Fuse Failed

Message Card Failure Raised

Severity Minor

Explanation There is a defective power fuse on the control module card in the specified slot.

Action Perform the following:

1. For simplex systems, replace the CFC card.
2. For duplex systems, swap activity, then replace the faulty card.
3. If the problem is still not resolved, contact Allied Telesis Technical Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC12	Degraded	Minor
•	CFC24	Degraded	Minor
•	CFC24	Degraded	Minor
•	CFC4	Degraded	Minor
•	CFC6	Degraded	Minor
•	CFC6	Degraded	Minor

2.14.7 SB 2.5v Power Failed

Message Card Failure Raised

Severity Critical

Explanation A problem has been detected with the 2.5v power output on the CFC24 switch board, affecting data packet processing. The CFC24 card is probably defective.

Action Perform the following:

1. Replace the CFC card.
2. If the problem is still not resolved, contact Allied Telesis Technical Support

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC24	Degraded	Critical
•	CFC24	Failed	Minor

2.14.8 SB CPU 2.5v Power Failed

Message Card Failure Raised

Severity Critical

Explanation A problem has been detected with the 2.5v power output for the CPU on the CFC24 switch board, affecting data packet processing. The CFC24 card is probably defective.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC24	Degraded	Critical
•	CFC24	Failed	Minor

2.14.9 SB 2.5v ANALOG Power Failed

Message Card Failure Raised

Severity Critical

Explanation A problem has been detected with the 1.25v analog power output on the CFC24 switch board, affecting data packet processing. The CFC24 card is probably defective.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC24	Degraded	Critical

• CFC24	Failed	Minor

2.14.10 SB 2.5v DIGITAL Power Failed

Message Card Failure Raised

Severity Critical

Explanation A problem has been detected with the 1.25v digital power output on the CFC24 switch board, affecting data packet processing. The CFC24 card is probably defective.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• CFC24	Degraded	Critical
• CFC24	Failed	Minor

2.14.11 Ring Generator Overload

Message Card Failure Raised

Severity Minor

Explanation Indicates that the ring generator on the card cannot handle the traffic demand.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• POTS24	Degraded	Minor

2.14.12 Ring Generator Failure

Message Card Failure Raised

Severity Minor

Explanation Indicates that the ring generator has stopped functioning. The problem may be due to traffic overload or could be that the card is defective and should be replaced.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	POTS24	Degraded	Major

2.14.13 Lost Communication with Call Server

Message Card Failure Raised

Severity Major

Explanation Indicates that the MGCP entity on the card cannot communicate with the external call agent. The problem could be with the Call Agent, other network factors external to the system, or could be due to a hardware or software condition with the POTS24 card itself.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	POTS24	Degraded	Major

2.14.14 DSP Failure

Message Card Failure Raised

Severity Minor

Explanation Indicates that the DSP (Digital Signal Processor) on the card is not functioning, which impacts the card's ability to packetize the analog voice waveform. Most likely the card is defective.

Action Perform the following:

1. Replace the card.

Alarms The following components are affected:

	Component	Status	Alarm
•	POTS24	Failed	Minor

2.14.15 Configuration Incomplete

Message Card Failure Raised

Severity Minor

Explanation Indicates that the IP, MGCP or RTP provisioning has not been completed for the card. Therefore, the card cannot provide service.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	POTS24	Failed	Minor

2.14.16 Hardware Unsupported

Message Card Failure Raised

Severity Info

Explanation The hardware version of the card is not supported by the system software.

Action Perform the following:

1. Replace the card with a newer version.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL	Failed	Minor
•	CES8	Failed	Major
•	NTE8	Failed	Major
•	POTS24 Card	Failed	Minor
•	SHDSL24	Failed	Minor

2.14.17 Incompatible with Active

Message Card Failure Raised

Severity Info

Explanation The hardware version of the inactive Control Module is incompatible with the hardware version of the active Control Module. Therefore, the Control Modules cannot sync.

Action Perform the following:

1. The inactive Control Module should be replaced with a version that matches the active one.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC24	Failed	Minor
•	CFC6	Failed	Minor

2.14.18 Internal Oscillator Failure

Message Card Failure Raised

Severity Minor

Explanation Not supported. [STILL TRUE?][To Be Supplied]

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	CES8	Degraded	Major
•	NTE8	Degraded	Major

2.14.19 Unable to Load

Message Card Failure Raised

Severity Minor

Explanation During syncing of the inactive Control Module with the active Control Module, the system was unable to load files from the active flash file system to the inactive flash file system. The problem may be due to the number of files on the active Control Module flash file system.

Action Perform the following:

1. Delete some of the files on the active Control Module flash file system.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC24	Failed	Major
•	CFC56	Failed	Major
•	CFC6	Failed	Major

2.14.20 DNS Server Timed Out

Message Card Failure Raised

Severity Minor

Explanation The IP protocol software on the card was not able to communicate with the DNS server to resolve the domain name of the peer (or the gateway) using the DNS protocol. This may indicate a problem with the DNS server or the intervening network, or the DNS server address may be invalid.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• POTS24	Degraded	Minor

2.14.21 ARP Resolution Failed

Message Card Failure Raised

Severity Minor

Explanation The IP protocol software on the card was not able to resolve the MAC address of the peer (or the gateway) using the ARP protocol. This may indicate that the peer (or the gateway) is down, or that the intervening network is down.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• POTS24	Degraded	Minor

2.14.22 DNS resolution failed

Message Card Failure Raised

Severity Minor

Explanation The IP protocol software on the card was not able to resolve the domain name of the peer (or the gateway) using the DNS protocol. This may indicate a problem with the DNS server, the domain name may be invalid, or there may be a problem with the intervening network.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• POTS24	Degraded	Minor

2.14.23 CFlash Failed

Message Card Failure Raised

Severity Minor

Explanation The system failed to access the compact flash media on the card. The media is probably bad or missing.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.14.24 AC Power A Failed

Message Card Failure Raised

Severity Minor

Explanation A shelf power failure on AC power feed A has been detected by the control module card in the specified slot. The problem could be due to the external power feed to the shelf, a defective AC power module, or the control module itself may be defective.

Action Perform the following:

1. In a duplex system, if alarm is on only one card, then replace the card.
2. Otherwise, verify power feed to shelf.
3. Replace AC power module.
4. Replace CFC card.
5. If the problem is still not resolved, contact Allied Telesis Technical Support.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.14.25 AC Power B Failed

Message Card Failure Raised

Severity Minor

Explanation A shelf power failure on AC power feed B has been detected by the control module card in the specified slot. The problem could be due to the external power feed to the shelf, a defective AC power module, or the control module itself may be defective.

Action Perform the following:

1. In a duplex system, if alarm is on only one card, then replace the card.

2. Otherwise, verify power feed to shelf.
3. Replace AC power module.
4. Replace CFC card.
5. If the problem is still not resolved, contact Allied Telesis Technical Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC12	Degraded	Minor

2.14.26 AC Power A Fan Failed

Message Card Failure Raised

Severity Minor

Explanation The power module controlling the AC power feed A has a fan failure. The most likely problem is the AC power module itself.

Action Perform the following:

1. Replace the AC power module.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC12	Degraded	Minor

2.14.27 AC Power B Fan Failed

Message Card Failure Raised

Severity Minor

Explanation The power module controlling the AC power feed B has a fan failure. The most likely problem is the AC power module itself.

Action Perform the following:

1. Replace the AC power module.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC12	Degraded	Minor

2.14.28 1.2v Power Failed

Message Card Failure Raised

Severity Critical

Explanation A problem has been detected with the 1.2v power output on the CFC12 switch board, affecting data packet processing. The CFC12 card is probably defective.

Action Perform the following:

1. Replace the CFC card.
2. If the problem is still not resolved, contact Allied Telesis Technical Support

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC12	Degraded	Critical
•	CFC200	Degraded	Critical
•	CFC200	Failed	Major

2.14.29 Duplicate IP Address

Message Card Failure Raised

Severity Major

Explanation The IP stack running in the card is reporting that it's IP address has been found duplicated somewhere in the same subnet. The card with the duplicate IP address may or may not be on the same shelf. Having duplicate IP addresses in the same subnet will affect communication within the subnet and may affect service.

Action Perform the following:

1. Use the SHOW IP INTERFACE command to query all interfaces on all shelves.
2. Use the SET IP INTERFACE command to modify the IP addresses (as necessary) so that they are all unique.

Alarms The following components are affected:

	Component	Status	Alarm
•	CES8	Degraded	Major
•	POTS24	Degraded	Major

2.14.30 IP buffer pool exhausted

Message Card Failure Raised

Severity Major

Explanation The IP stack in the card is receiving more packets than it can handle. The condition is most likely affecting service. The problem will clear itself when the traffic level decreases.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	CES8	Degraded	Major
•	POTS24	Degraded	Major

2.14.31 Power Input Incompatibility

Message Card Failure Raised

Severity Minor

Explanation This degrading alarm indicates that the card is incompatible with the input power source supplied. For example, older iMAP card versions are only compatible with 48v power sources.

Action Perform the following:

1. To clear the alarm, either change the power source or upgrade the card with a newer model that supports the alternative power source.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL	Degraded	Minor
•	CES8	Degraded	Minor
•	CFC12	Degraded	Minor
•	CFC24	Degraded	Minor
•	CFC24	Degraded	Minor
•	CFC6	Degraded	Minor
•	CFC6	Degraded	Minor
•	EPON2	Degraded	Minor
•	FE10	Degraded	Minor
•	FE2	Degraded	Minor
•	FX10	Degraded	Minor
•	GE	Degraded	Minor
•	GE	Degraded	Minor
•	GE Virtual Card	Degraded	Minor
•	GE Virtual Card	Degraded	Minor
•	NTE8	Degraded	Minor

• POTS24	Degraded	Minor
• SHDSL24	Degraded	Minor
• XE	Degraded	Minor
• XE	Degraded	Minor

2.14.32 Inconsistent Flooding

Message Card Failure Raised

Severity Info

Explanation When IGMP is enabled on an EPON interface, unknown Multicast is blocked. The EPON interface will not flood any unknown multicast on any VLAN, except 256 “well known” groups. This behavior is unlike other IGMP supporting interfaces on the iMAP. Since the FLOODUNKNOWN attribute is a system setting, there is nothing to prevent the user from having a setting that is inconsistent with an EPON2 card. When the setting is inconsistent an “Inconsistent Flooding” degrading alarm is present on the card. If the user changes the setting to be inconsistent, the alarm provides immediate feedback that the setting is inconsistent with the card type.

Action Perform the following:

1. To clear this alarm, change the FLOODUNKNOWN attribute setting to OFF (which is the default).

Alarms The following components are affected:

Component	Status	Alarm
• EPON2	Degraded	Major

2.14.33 Card Disable Failed

Message Card Failure Raised

Severity Info

Explanation No response from an attempt to disable the card. With POTS, the disable is supposed to terminate the call processing entity on the card. This is usually caused by communication errors with the call server. Note that the user can restart the card while it’s disabled to ensure that all functions on the card are terminated.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm

• POTS24	Online	Info

2.14.34 Protocol Mismatch

Message: Card Failure Raised

Severity: Info

Explanation: The PROTOCOL attribute on the POTS card (MGCP or SIP) doesn't match the load running on the card (POTS24 or POTS24S).

Action: Perform the following:

1. Change the prefload to match.
2. Or change the protocol attribute to match the load type.

Alarms: The following components are affected:

	Component	Status	Alarm
•	POTS24	Failed	Minor

2.14.35 Incompatible Load

Message: Card Failure Raised

Severity: Info

Explanation: The Incompatible Load alarm is raised when the SM is running a load that the CFC does not support. For example, this alarm is raised if the CFC is running 9.0.x and the SM is running 7.x.x, 9.1.x or 10.0.x. This alarm is a failing alarm for the SM; the card cannot be put into service.

Action: Perform the following:

1. To Be Supplied

Alarms: The following components are affected:

	Component	Status	Alarm
•	ADSL	Failed	Minor
•	CES8	Failed	Major
•	EPON2	Failed	Major
•	FE10	Failed	Minor
•	FX10	Failed	Minor
•	GE	Failed	Major
•	NTE8	Failed	Major
•	POTS24	Failed	Minor

• SHDSL24	Failed	Minor
• VDSL24	Failed	Minor

2.14.36 Unsupported Hardware

Message: Card Failure Raised

Severity: Minor

Explanation: A card has been installed that is not supported by 15.0 software (e.g., ADSL16, ADSL8s, ADSL16B, SHDSL16).

Action: Perform the following:

1. To Be Supplied

Alarms: The following components are affected:

Component	Status	Alarm
• ADSL	Failed	Minor
• SHDSL	Failed	Minor

2.15 CARD023 - atnCardDefectRaised

2.15.1 Sync Card Not Detected

Message: Card Info Alarm Raised

Severity: Major

Explanation: An ADSL16C [STILL TRUE?] [TO BE SUPPLIED] card has been inserted into the Telesyn MAP 7000 shelf, and in the shelf there is no CFC with an Annex C component (mezzanine card) on either the active or inactive side. As a result, the shelf cannot provide Annex C service for the ADSL16C card.

Action: Perform the following:

1. To Be Supplied

Alarms: The following components are affected:

Component	Status	Alarm
• CFC6	Online	Major

2.15.2 Loss of Primary Reference

Message: Card Info Alarm Raised

Severity: Major

Explanation The Primary Timing Source (from the Network through the FAN8 component) for the CFC6-C card is unavailable. (In a 7700, this network clock source terminates on both the active and inactive CFC-6 cards.) There is therefore only one clock source available for the timing references needed for correct AnnexC service.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC6	Online	Major

2.15.3 Loss of Secondary Reference

Message Card Info Alarm Raised

Severity Major

Explanation The Secondary Timing Source (from the Network through the FAN8 component) for the CFC6-C card is unavailable. (In a 7700, this network clock source terminates on both the active and inactive CFC-6 cards.) There is therefore only one clock source available for the timing references needed for correct AnnexC service.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC6	Online	Major

2.15.4 Loss of Holdover

Message Card Info Alarm Raised

Severity Minor

Explanation The mezzanine card on the CFC6-C is no longer in holdover and can no longer provide timing. As a result, the shelf cannot provide AnnexC service for the ADSL16C card. The inactive CFC-C (if present) may still be able to provide AnnexC service following a switchover.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC6	Online	Major

2.15.5 Sync Card Clock Error

Message `Card Info Alarm Raised`

Severity `Major`

Explanation `The mezzanine card on the CFC6-C has failed and can no longer provide timing. As a result, the shelf cannot provide AnnexC service for the ADSL16C card. The inactive CFC-C (if present) may still be able to provide AnnexC service following a switchover.`

Action `Perform the following:`

1. To Be Supplied

Alarms `The following components are affected:`

	Component	Status	Alarm
•	CFC6	Online	Major

2.16 CARD046 - ATNCARDFDBMGMTOVERFLOW

2.16.1 Not Applicable

Message `FDB Management Overflow.`

Severity `Info`

Explanation `The MAC learning limit of the card has been temporarily exceeded due to some network condition. No other MACs can be learned (written to the FDB) until the ageing timer has expired to make room in the FDB. This log is generated by the FE10.`

Action `Perform the following:`

1. No action is required [Still True?] [To Be Supplied].

Alarms `The following components are affected:`

	Component	Status	Alarm
•	None		

2.17 CUC001 - atnCUCFaultRaised

2.17.1 Not Present

Message Cooling Unit Controller Failure Raised

Severity Critical

Explanation The cooling unit controller is not present in the shelf.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	FC7	Not installed	Major

2.17.2 Power Supply Failure

Message Cooling Unit Controller Failure Raised

Severity Critical

Explanation The power supply for the cooling unit controller has failed.

1. Replace the fan controller card.

Alarms The following components are affected:

	Component	Status	Alarm
•	FC7	Degraded	Minor

2.17.3 No Communication

Message Cooling Unit Controller Failure Raised

Severity Critical

Explanation The system cannot communicate with the cooling unit controller.

Action Perform the following:

1. Reseat the card.
2. If the alarm persists, replace the card.

Alarms The following components are affected:

	Component	Status	Alarm
•	FC7	Failed	Major

2.18 FAN001 - atnCUCFaultRaised

2.18.1 Hardware Not Recognized

Message Cooling Unit Controller Failure Raised

Severity Critical

Explanation The system does not recognize the hardware type that is physically present in the cooling unit controller slot.

Action Perform the following:

1. Reseat the card.
2. If the alarm persists, replace the card.

Alarms The following components are affected:

	Component	Status	Alarm
•	FC7	Failed	Major

2.19 FAN001 - atnFanFaultRaised

2.19.1 Fan Module Power Supply Failure

Message Fan Module Failure Raised

Severity Critical

Explanation The power supply for the fan module has failed.

Action Perform the following:

1. Remove the fan module and check for dust or dirt.
2. Clean the fan module, if required, and reinsert it into the system.
3. If the alarm returns, replace the card.

Alarms The following components are affected:

	Component	Status	Alarm
•	FAN8	Degraded	Minor
•	FM7	Degraded	Minor

2.20 INTF001 - Linkdown

2.20.1 All parents non-administratively down

Message Interface Fault Set

Severity Major

Explanation All of the parent PPPs that are associated with the MLPPP are not available, and so all traffic on the MLPPP (a combining of two to eight DS1s/E1s) cannot be passed.

Action Perform the following:

1. Check the status of the NTE8 card, DS1 interfaces, and the PPPs.

Alarms The following components are affected:

	Component	Status	Alarm
•	MLPPP	Failed	Major

2.20.2 Config Failed

Message Interface Fault Set

Severity Major

Explanation The interface failed to configure. This could be due to high traffic through the card, a problem with provisioning associated with the interface, or could be due to running an incompatible software release in the associated card. For the DS3, a DS3 SFP is present, but could not be configured for some reason. The DS3 interface will be failed. The state of the associated GE interface depends on whatever configuration is already present on the DS3 SFP.

Action Perform the following:

1. Verify traffic capacity.
2. Verify load preferences.
3. Verify provisioning.

Alarms The following components are affected:

	Component	Status	Alarm
•	ATMBOND	Failed	Info
•	DS3	Failed	Major
•	MLPPP	Failed	Major
•	ONU	Failed	Major
•	PPP	Failed	Major

2.20.3 Echo Request Timeout

Message Interface Fault Set

Severity Major

Explanation The PPP/MLPPP protocol periodically checks its integrity by using echo requests, where it sends a message to the peer and expects the peer to reply. Consistent failure to receive the echo reply within a given time period will cause the interface to fail with this alarm. The echo request timeout value is configurable and can be changed using the SET INTERFACE command if desired.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	MLPPP	Failed	Major
•	PPP	Failed	Major

2.20.4 Loopback Detected

Message Interface Fault Set

Severity Major

Explanation The PPP/MLPPP protocol has detected a loopback condition using its echo request mechanism. Since it is not communicating with the peer, the interface is failed with this alarm.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	MLPPP	Failed	Major
•	PPP	Failed	Major

2.20.5 Negotiation Failed

Message Interface Fault Set

Severity Major

Explanation The interface has timed out in its attempt to negotiate link parameters with its peer. More debugging information can be obtained by getting event logs, using the ADD TRACE and SHOW TRACE commands.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	MLPPP	Failed	Major
•	PPP	Failed	Major

2.20.6 Peer Disabled

Message `Interface Fault Set`

Severity `Major`

Explanation `The remote peer has gracefully taken the link down, but the local interface is still enabled. A common cause would be that the remote interface has been administratively disabled.`

Action `Perform the following:`

1. To Be Supplied.

Alarms `The following components are affected:`

	Component	Status	Alarm
•	MLPPP	Failed	Major
•	PPP	Failed	Major

2.20.7 ONU Not Discovered

Message `Not Applicable`

Severity `Minor`

Explanation `This alarm indicates that no logical links have been discovered for a pre-provisioned ONU.`

Action `Perform the following:`

1. Check that the ONU is connected to the fiber.
2. If ONU is connected, make sure it is powered up.
3. If the alarm persists, replace the defective ONU.

Alarms `The following components are affected:`

	Component	Status	Alarm
•	ONU	Failed	Info

2.20.8 Remote Tranmsit Failed

Message `Interface Fault Set`

Severity `Info`

Explanation This failing alarm is the result of the ONU failing to transmit on the EPON, and is triggered by hardware inputs from transceiver. The transmitted output does not input as reported by the EPON optics. This alarm may indicate a problem with the ONU or its connection to the fiber.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	ONU	Failed	Info

2.20.9 Loading Firmware

Message Interface Fault Set

Severity Info

Explanation The EPON card software load file also contains firmware for both the OLT and ONU. This alarm indicates that the firmware on the ONU is being upgraded, as an automatic result of upgrading the EPON card's software load.

Action Perform the following:

1. No action [Still True?] [To Be Supplied]. The alarm should clear on its own when the upgrade is completed.

Alarms The following components are affected:

	Component	Status	Alarm
•	ONU	Failed	Info

2.20.10 Waiting to Load Firmware

Message Interface Fault Set

Severity Info

Explanation The EPON card software load file also contains firmware for both the OLT and ONU. This alarm indicates that the firmware on the ONU is to be upgraded, as an automatic result of upgrading the EPON card's software load. Per EPON interface, only one ONU at a time is upgraded, all the rest are held in queue with this alarm raised against them. When the ONU starts its firmware upgrade, this alarm is cleared and the "Loading Firmware" alarm is raised.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	ONU	Failed	Info

2.20.11 Not Applicable

Message New root trap

Severity Info

Explanation To Be Supplied.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	None		

2.20.12 All Links Failed

Message Interface Fault Set

Severity Info

Explanation The ONU is not configured because none of the links (VLANs) have been discovered, so it's not traffic capable in this state. Since no links on one ONU cannot be discovered, it is probable that all links for all ONUs for the EPON interface have failed (Up to 192, or 32x6, links).

Action Perform the following:

1. Check the EPON card and interface.

Alarms The following components are affected:

	Component	Status	Alarm
•	ONU	Failed	Major

2.20.13 Unexpected BPDU Received

Message Interface Fault Set

Severity Info

Explanation This failing alarm is raised when a BPDU is received on an interface that has BPDU cop feature enabled. The BPDU cop feature protects

the iMAP from network loops and other threats where the symptom is reception of an unexpected BPDU.

Action Perform the following:

1. To clear alarm, disable and re-enable the interface.

Alarms The following components are affected:

	Component	Status	Alarm
•	ATMBOND	AutoDisabled	Info
•	MLPPP	AutoDisabled	Major
•	ONU	AutoDisabled	Info
•	PPP	AutoDisabled	Major

2.20.14 Report Timeout

Message Interface Fault Set

Severity Info

Explanation This alarm is raised when the ONU does not respond to grants from the OLT. This is usually caused by disconnecting the fiber at the ONU or by powering down the ONU, and in those cases this alarm will eventually be masked by the “All links down” alarm on the ONU.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	ONU	Failed	Info

2.20.15 Links Not Discovered

Message Interface Fault Set

Severity Major

Explanation Prior to release 9.0, this alarm on the ONU was a degrading alarm. This implied that the ONU could be carrying traffic on any subset of its 6 links that are discovered. However, in 9.0 the ONU is not even configured unless all links have been discovered, so it's not traffic capable in this state. Therefore, this alarm is failing with the same severity and impact as "All Links Failed".

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	ONU	Failed	Info

2.20.16 All ASM Links Down

Message: Interface Fault Set

Severity: Info

Explanation: The ATMBOND is failed because all of the internal links for communicating Asynchronous Status Messages (ASM) are not functioning. Resolving this problem may involve any one or combination of the action listed below.

Action: Perform the following:

1. Reset the G.bond modem at the CPE.
2. Disable/Enable the ATMBOND.
3. Disable/Enable the individual ADSL interfaces in the ATMBOND group.

Alarms: The following components are affected:

	Component	Status	Alarm
•	ATMBOND	Failed	Info

2.20.17 All Parent Interfaces Down

Message: Interface Fault Set

Severity: Info

Explanation: The ATMBOND group is failed because all of the ADSL interfaces in the group are either failed or disabled.

Action: Perform the following:

1. To Be Supplied.

Alarms: The following components are affected:

	Component	Status	Alarm
•	ATMBOND	Failed	Info

2.20.18 Loss of Signal (LOS)

Message: Interface Fault Set

Severity: Major

Explanation: A Loss of Signal condition has been detected on the DS3.

Action: Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	DS3	Failed	Major

2.20.19 Alarm Indication Signal

Message Interface Fault Set

Severity Info

Explanation An Alarm Indication Signal has been received by the DS3. This is sent from the remote peer to indicate that a transmission interruption has been detected in the network. One common reason for AIS is when the remote peer has been administratively disabled.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	DS3	Failed	Major

2.20.20 SFP Type Mismatch

Message Interface Fault Set

Severity Info

Explanation An SFP is present, but it is not a DS3 SFP. The condition of the associated GE interface depends on the peer configuration.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	DS3	Failed	Major

2.20.21 SFP Not Present

Message Interface Fault Set

Severity Info

Explanation No SFP (of any kind) is physically present in the GE port. The associated GE interface is therefore also failed.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	DS3	Failed	Major

2.20.22 Receive Loss of Lock

Message Interface Fault Set

Severity Info

Explanation The DS3 has detected a Loss of Lock condition on its incoming signal, possibly due to problems with the incoming reference clock signal.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	DS3	Failed	Major

2.20.23 Remote Defect Indication

Message Interface Fault Set

Severity Info

Explanation A Remote Defect Indication has been received by the DS3, indicating that the remote end of the DS3 has detected a failure in it's incoming signal.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	DS3	Failed	Major

2.21 INTF003 - Unknown

2.21.1 Bandwidth Degraded

Message Interface Degradation Set

Severity Minor

Explanation One or more of the parent PPPs of the affected MLPPP is not passing traffic, but the MLPPP is still providing limited service because there is bandwidth available through the other PPPs. The DS1/E1 or corresponding PPP interface(s) may have failed, or may have been administratively disabled.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	MLPPP	Degraded	Minor

2.22 INTF003 - atnInterfaceDefectRaised

2.22.1 Keep Alive Timeout

Message Not Applicable

Severity Info

Explanation This degrading alarm is reported by the OLT (represented by the EPON interface) on behalf of the ONU. The alarm is raised per logical link on the ONU, and indicates that the OAM layer running on the OLT is not receiving periodic messages from its peer on the ONU. This alarm is usually the result of mis-configuration of the EPON bandwidth, causing insufficient bandwidth for normal OAM communication. The QOS policy configuration limits enforced by the iMAP CLI should prevent this alarm from occurring due to mis-configuration. Therefore, the presence of this alarm should be rare.

Action Perform the following:

1. Disable/enable the ONU.
2. Disable/enable the EPON interface.
3. Disable/enable the EPON card.
4. Power reset the ONU.
5. Replace the ONU.
6. Replace the EPON card.

Alarms The following components are affected:

	Component	Status	Alarm
•	ONU	Degraded	Info

2.22.2 Remote Loss of Signal (UNI)

Message Not Applicable

Severity Info

Explanation This degrading alarm against the ONU indicates a loss of signal condition on the UNI side of the ONU.

Action Perform the following:

1. Make sure a device is connected to the UNI interface on the ONU.
2. If a device is connected to the UNI interface, make sure it is powered up.
3. Check to see if the device or cable connected to the UNI interface is not defective. If so, replace the defective device/cable.
4. Check to see if the ONU itself is defective. If so, replace it.

Alarms The following components are affected:

	Component	Status	Alarm
•	ONU	Degraded	Info

2.22.3 Remote Gate Timeout

Message Not Applicable

Severity Info

Explanation This degrading alarm is raised per logical link against the ONU, and is the result of excessive interval between MPCP gates.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	ONU	Degraded	Info

2.22.4 Remote Keep Alive Timeout

Message Not Applicable

Severity Info

Explanation This degrading alarm is raised per logical link on the ONU, and indicates that the OAM layer running on the ONU is not receiving periodic messages from its peer on the OLT. This alarm is usually the result of mis-configuration of the EPON bandwidth, causing insufficient bandwidth for normal OAM communication. The QOS policy configuration limits enforced by the iMAP CLI should prevent this

alarm from occurring due to mis-configuration. Therefore, presence of this alarm should be rare.

Action Perform the following:

1. Disable/enable the ONU.
2. Disable/enable the EPON interface.
3. Disable/enable the EPON card.
4. Power reset the ONU.
5. Replace the ONU.
6. Replace the EPON card.

Alarms The following components are affected:

	Component	Status	Alarm
•	ONU	Degraded	Info

2.22.5 Mismatched ONU Type

Message To Be Supplied

Severity Info

Explanation The ONU is pre-provisioned as either TK3711 or TK3713, but the ONU physically plugged in to the EPON is the other type.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	ONU	Degraded	Info

2.22.6 Unsupported ONU Type

Message To Be Supplied

Severity Info

Explanation ONU is pre-provisioned as either TK3711 or TK3713, but the ONU physically plugged into the EPON is neither type.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	ONU	Degraded	Info

2.22.7 No Response from BRAS

Message Not Applicable

Severity Info

Explanation The PPPoE session cannot be established. A timeout has occurred while waiting for the PADO form the BRAS server. The associated alarm shows which VC is affected by the alarm. If the PADO is never received, the protocol handshake must begin again.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL Port	Degraded	Info
•	SHDSL Port	Degraded	Info
•	VDSL Port	Degraded	Info

2.22.8 Negotiation Failed

Message Not Applicable

Severity Info

Explanation The PPPoE session cannot be established. An error was reported be the BRAS server in either the PADO or PADS message. The session establishment process must begin again.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL Port	Degraded	Info
•	SHDSL Port	Degraded	Info
•	VDSL Port	Degraded	Info

2.22.9 Echo Request Timeout

Message Not Applicable

Severity Minor

Explanation The PPPoE session cannot be established. An echo timeout occurred while in the session open state. The associated alarm shows which

VC is affected by the alarm. In this case, the session must begin again (transition to PADI state.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• ADSL Port	Degraded	Info
• SHDSL Port	Degraded	Info
• VDSL Port	Degraded	Info

2.22.10 Below Min Downstream Aggregate Rate

Message Interface Degradation Set

Severity Info

Explanation The cumulative total of the actual downstream rates achieved by all of the interfaces in the ATMBOND group is less than the minimum downstream aggregate rate that is provisioned for the ATMBOND.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• ATMBOND	Degraded	Info

2.22.11 Below Min Upstream Aggregate Rate

Message Interface Degradation Set

Severity Info

Explanation The cumulative total of the actual upstream rates achieved by all of the interfaces in the ATMBOND group is less than the minimum upstream aggregate rate that is provisioned for the ATMBOND.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• ATMBOND	Degraded	Info

2.22.12 Downstream Differential Rate Exceeded

Message Interface Degradation Set

Severity Info

Explanation One of the ADSL interfaces in the ATMBOND group has achieved a downstream rate that is less than 25% of the downstream rate achieved by the companion interface in the group.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	ATMBOND	Degraded	Info

2.22.13 Some ASM Links Down

Message Interface Degradation Set

Severity Info

Explanation The ATMBOND is degraded because some of the internal links for communicating Asynchronous Status Messages (ASM) are not functioning. Resolving this problem may involve any one or combination of the actions listed below.

Action Perform the following:

1. Reset the G.bond modem at the CPE.
2. Disable/Enable the ATMBOND.
3. Disable/Enable the individual ADSL interfaces in the ATMBOND group.

Alarms The following components are affected:

	Component	Status	Alarm
•	ATMBOND	Degraded	Info

2.22.14 Some Parent Interfaces Down

Message Interface Degradation Set

Severity Info

Explanation The ATMBOND group is degraded because one of the ADSL interfaces in the group is either failed or disabled.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	ATMBOND	Degraded	Critical

2.22.15 Status Attribute

Message To Be Supplied

Severity Info

Explanation To Be Supplied.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	ATMBOND	Degraded	Info

2.22.16 Upstream Differential Rate Exceeded

Message Interface Degradation Set

Severity Minor

Explanation One of the ADSL interfaces in the ATMBOND group has achieved an upstream rate that is less than 25% of the upstream rate achieved by the companion interface in the group.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	ATMBOND	Degraded	Info

2.22.17 Excessive Zeroes

Message Interface Degradation Set

Severity Info

Explanation Excessive zero's have been detected in the incoming signal of the DS3.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	DS3	Degraded	Info

2.22.18 Bipolar Violation

Message Interface Degradation Set

Severity Info

Explanation Bipolar violations have been detected on the incoming signal of the DS3.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	DS3	Degraded	Info

2.22.19 Far-End SEF AIS

Message Interface Degradation Set

Severity Info

Explanation Severely Errored Frame (SEF) or Alarm Indication Signal (AIS) has been received by the remote peer of the DS3.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	DS3	Degraded	Info

2.22.20 Out of Frame

Message Interface Degradation Set

Severity Info

Explanation Framing errors have been detected on the incoming signal of the DS3.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	DS3	Degraded	Info

2.23 INTF003 - Linkdown

2.23.1 Loss of Frame (LOF)

Message Port Fault Set

Severity Minor

Explanation The port has lost the framing source from the far end equipment.

Action Perform the following:

1. Verify framing source.
2. Verify far-end equipment.
3. Disable/enable port.

Alarms The following components are affected:

	Component	Status	Alarm
•	DS3	Degraded	Info

2.24 PMON001 - atnDs1CurrentLCVThreshTrap

2.24.1 Not Applicable

Message Not Applicable

Severity Minor

Explanation The number of Line Coding Violations exceeds the provisioned threshold for the current 15-minute period.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

	Component	Status	Alarm
•	None		

2.25 PMON002 - atnDs1CurrentLESThreshTrap

2.25.1 Not Applicable

Message Not Applicable

Severity Minor

Explanation The number of link errored seconds condition exceeds the provisioned threshold for the current 15-minute period.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.26 PMON003 - atnDs1CurrentLOSThreshTrap

2.26.1 Not Applicable

Message Not Applicable

Severity Minor

Explanation The number of Loss of Signal conditions exceeds the provisioned threshold for the current 15-minute period.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.27 PMON004 - atnDs1CurrentSESThreshTrap

2.27.1 Not Applicable

Message Not Applicable

Severity Minor

Explanation The number of Severely Error Seconds condition exceeds the provisioned threshold for the current 15-minute period.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.28 PMON005 - atnDs1DayUASThreshTrap

2.28.1 Not Applicable

Message Not Applicable

Severity Minor

Explanation The number of Unavailable Seconds condition exceeds the provisioned threshold for the current 15-minute period.

Action Perform the following:

1. To Be Supplied.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.29 PORT003 - Linkdown

2.29.1 CAS Thermal Shutdown

Message Port Fault Set

Severity Minor

Explanation The CAS (Card Access Switch) for this port has shutdown due to high temperature. This could be the result of external voltage on the line or could be due to a defective card that needs replacing.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• POTS Port	Failed	Minor

2.29.2 SLIC Thermal Shutdown

Message Port Fault Set

Severity Minor

Explanation The SLIC (Subscriber Line Interface Circuit) on the card for this port has shutdown due to high temperature.

Action Perform the following:

1. Replace card.

Alarms The following components are affected:

	Component	Status	Alarm
•	POTS Port	Failed	Minor

2.29.3 AC Fault

Message Port Fault Set

Severity Minor

Explanation Indicates that external AC voltage has been detected on the line. Most likely the fault is due to an external stimulus (fault on the external line itself).

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	POTS Port	Failed	Minor

2.29.4 DC Fault

Message Port Fault Set

Severity Minor

Explanation Indicates that external DC voltage has been detected on the line. Most likely the fault is due to an external stimulus (fault on the external line itself).

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	POTS Port	Failed	Minor

2.29.5 PCM Clock Failure

Message Port Fault Set

Severity Minor

Explanation The PCM (Pulse Code Modulation) clock that applies timing for digital encoding of the analog line waveform is defective.

Action Perform the following:

1. Replace card.

Alarms The following components are affected:

	Component	Status	Alarm
•	POTS Port	Failed	Minor

2.29.6 Battery Failure

Message Port Fault Set

Severity Minor

Explanation The battery that applies line voltages is defective.

Action Perform the following:

1. Replace card.

Alarms The following components are affected:

	Component	Status	Alarm
•	POTS Port	Failed	Minor

2.29.7 No Peer Present (NPP)

Message Port Fault Set

Severity Info

Explanation Same as Loss of Signal (LOS). The port is no longer receiving a signal from the far end equipment.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL Port	Failed	Info
•	SHDSL Port	Failed	Info

2.29.8 Loopback Failed

Message Port Fault Set

Severity Minor

Explanation The provisioned loopback configuration could not be applied to the hardware.

Action Perform the following:

1. Set the loopback configuration back to "NONE" and try again.

Alarms The following components are affected:

	Component	Status	Alarm
•	DS1 Port	Failed	Major
•	E1 Port	Failed	Major

2.29.9 Timing Reference Failed

Message Port Fault Set

Severity Minor

Explanation Not supported in R5.0. [Still True?] [To Be Supplied]

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	DS1 Port	Failed	Major
•	E1 Port	Failed	Major

2.29.10 Link Quality Failed

Message Port Fault Set

Severity Major

Explanation Some services that are carried across an MLPPP interface are especially sensitive to packet loss, thus action must be taken to move traffic off of a physical interface without waiting for it's defects to soak into faults (typically 2.5 seconds). It is possible for transient failures to cause the physical interface to be removed from service while the "normal" alarms (e.g. LOS, LOF) are never completely soaked, so this specialized alarm is raised on the physical interface to immediately indicate to the user that it has been removed from service.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	DS1 Port	Failed	Major
•	E1 Port	Failed	Major

2.29.11 Loss of RTP Receive Stream

Message Port Fault Set

Severity Minor

Explanation The POTS card has detected that it is not receiving RTP packets as expected for the interface. The RTP packets have been interrupted or are not being sent from the call agent.

Action Perform the following:

1. Check for an external network condition (failure or capacity).
2. If no problem is found with the external network or call agent, disable/enable the interface.

Alarms The following components are affected:

	Component	Status	Alarm
•	POTS Port	Degraded	Minor

2.29.12 Loss of RTP Transmit Stream

Message Port Fault Set

Severity Minor

Explanation The POTS card has detected that it is not transmitting RTP packets as expected for the interface. The problem is most likely due to an internal resource error on the POTS card.

Action Perform the following:

1. Disable/enable the interface.

Alarms The following components are affected:

	Component	Status	Alarm
•	POTS Port	Failed	Minor

2.29.13 Receiving AIS

Message Port Fault Set

Severity Major

Explanation The physical interface has detected an Alarm Indication Signal from the remote peer as per ANSI T1.231. AIS is generated by the remote peer when it detects a LOS defect, or when it has been placed in maintenance state. A common cause of this alarm is when the remote peer has been administratively disabled. For more information see ANSI T1.403-1999 Annex J.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	DS1 Port	Failed	Major
•	E1 Port	Failed	Major

2.29.14 Receiving RAI

Message Port Fault Set

Severity Major

Explanation The physical interface is failed because it received a Remote Alarm Indication from its remote peer. RAI is sent from remote peer when it detects that it has lost the incoming signal.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	DS1 Port	Failed	Major
•	E1 Port	Failed	Major

2.29.15 Transmit Failed

Message Port Fault Set

Severity Major

Explanation This failing alarm is the result of the OLT failing to transmit on the EPON, and is triggered by hardware inputs from transceiver. The transmitted output does not input as reported by the EPON optics. This alarm may indicate a problem with the EPON card or the SFP connecting with the fiber.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	EPON Port	Failed	Major

2.29.16 No Links Discovered

Message Port Fault Set

Severity Major

Explanation This alarm indicates that no logical links have been discovered for any ONU on the EPON interface.

Action Perform the following:

1. Verify that fiber is connected to the EPON interface.
2. Verify that ONUs are connected to the fiber.
3. If ONUs are connected to the fiber, make sure they are powered up.
4. Check to see if the fiber is defective. If so, replace fiber.
5. Check to see if the EPON card is defective. If so, replace EPON.

Alarms The following components are affected:

	Component	Status	Alarm
•	EPON Port	Failed	Major

2.29.17 Loading Firmware

Message Port Fault Set

Severity Major

Explanation The EPON card software load file also contains firmware for both the OLT and ONU. This alarm indicates that the firmware on the OLT is being upgraded, as part of upgrading the EPON card's software load. Since the firmware upgrade occurs during the card upgrade itself while the EPON interface is in the dependency state, the user should never see this alarm.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	EPON Port	Failed	Major

2.29.18 Interface Internal Failure

Message Port Fault Set

Severity Minor

Explanation The internal interface between the OLT and ONU has failed.

Action Perform the following:

1. Reset the OLT (enable/disable).

Alarms The following components are affected:

	Component	Status	Alarm
•	EPON Port	Failed	Major

2.29.19 Registration Failed

Message Port Fault Set

Severity Info

Explanation The registration failure alarm is set when a POTS PORT loses its registration status with the call agent, signaling that a port is out of service. The fault is cleared when the registration is restored.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	POTS Port	Failed	Minor

2.29.20 DS3 Out of Service

Message Port Fault Set

Severity Major

Explanation The GE port is using DS3 SFP and the associated DS3 is provisioned, but the DS3 is failed.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	None		

2.30 PORT005 - HDSL2SHDSLPERFLOSWSTHRESH

2.30.1 Loss Of Sync Word

Message Port Fault Set

Severity Info

Explanation The port is having difficulty syncing with the far end equipment.

Action Perform the following:

1. Verify far-end equipment.
2. Disable/enable port.

Alarms The following components are affected:

	Component	Status	Alarm
•	SHDSL Port	Degraded	Info

2.31 PORT005 - atnPortDefectRaised

2.31.1 Loss Of Signal Quality (LOSQE)

Message Port Fault Set

Severity Info

Explanation The port is receiving low signal quality from the far end equipment, but is still able to pass some payload.

Action Perform the following:

1. Verify far-end equipment.
2. Disable/enable port.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL Port	Online	None
•	SHDSL Port	Online	None
•	VDSL Port	Degraded	Info

2.31.2 Loss of Power - Modem Off (LPR)

Message Port Fault Set

Severity Info

Explanation Modem power has been disconnected.

Action Perform the following:

1. Verify far-end equipment.
2. Disable/enable port.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL Port	Degraded	Info

- SHDSL Port Degraded Info
- VDSL Port Degraded Info

2.31.3 Transmit Degraded

Message Port State Change

Severity Major

Explanation This degrading alarm is the result of the OLT having errors transmitting on the EPON, and is triggered by hardware inputs from transceiver. The transmitted output has a high error level, but not so high as to cause failure. This alarm may indicate a problem with the EPON card or the SFP connecting with the fiber.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• EPON Port	Degraded	Major

2.31.4 Downstream Bandwidth Resources Exceeded

Message To Be Supplied

Severity Major

Explanation The user has configured ONUs with QOS policies such that the total of the minimum downstream bandwidths has exceeded the capacity of the associated EPON interface.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• EPON Port	Degraded	Major

2.31.5 Bandwidth Priority Category Resources Exceeded

Message To Be Supplied

Severity Major

Explanation The user has configured ONUs with QOS policies that have exceeded the priority allocation capacity of the associated EPON interface. Priority are assigned based on minimum bandwidth and delay sensi-

tivity. There are 3 categories: 1. delay sensitive 2. delay tolerant but non-zero minimum bandwidth 3. delay tolerant with zero minimum bandwidth (aka "best effort") Each category has limits on how many logical links can be included.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	EPON Port	Degraded	Major

2.31.6 Link Threshold Exceeded

Message Not Applicable

Severity Info

Explanation A threshold has been crossed (LINK THRESHOLD EXCEEDED) in configuring the ONU links.

Action Perform the following:

1. Reset the OLT (disable/enable the port) during the next convenient time.

Alarms The following components are affected:

	Component	Status	Alarm
•	EPON Port	Online	Info

2.32 PORT005 - Linkdown

2.32.1 Loss of Cell Delineation

Message Port Fault Set

Severity Info

Explanation A persistent condition is present that prevents the port from delineating cells received from the far-end.

Action Perform the following:

1. Verify that the provisioning characteristics of the port match those of the device to which it is attached.
2. If there are any differences, correct them.
3. If there are no differences, attempt disabling and then re-enabling the port to see if the problem persists.
4. If the problem persists, contact Allied Telesis Technical Support.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL Port	Failed	Info
•	SHDSL Port	Failed	Info

2.33 PORT005 - Not applicable

2.33.1 Timing Reference Degraded

Message Port Degradation Set

Severity Minor

Explanation The port's provisioned timing reference cannot provide a reliable timing reference. The interface is being timed from an alternate reference that is not known to be locked to the provisioned source.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

	Component	Status	Alarm
•	DS1 Port	Degraded	Minor
•	E1 Port	Degraded	Minor

2.34 PORT005 - atnPortDefectCleared

2.34.1 Upstream Bandwidth Resources Exceeded

Message To Be Supplied

Severity Major

Explanation The user has configured ONUs with QOS policies such that the total of the minimum upstream bandwidths has exceeded the capacity of the associated EPON interface.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

	Component	Status	Alarm
•	EPON Port	Degraded	Major

2.35 PORT013 - Not applicable

2.35.1 High priority queue overflow

Message Port Information

Severity Info

Explanation Traffic mapped to high priority queue(s) by the provisioned QoS configuration is causing queue overflows, which results in dropped packets. To remedy this, map less traffic to high priority queues.

Action Perform the following:

1. Verify the QOS/traffic configuration for the port.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL Port	Online	None
•	SHDSL Port	Online	None

2.36 PORT013 - To Be Supplied

2.36.1 Port AIS Received

Message Port Information

Severity Info

Explanation Not supported in R5.0. [STILL TRUE?][To Be Supplied]

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

	Component	Status	Alarm
•	DS1 Port	Online	None
•	E1 Port	Online	None

Note: This is only logged. It does not show up as an alarm. On a SHOW PORT, it will display as a runtime attribute.

2.37 PORT017 - Not applicable

2.37.1 Not Applicable

Message EC changed from ON to OFF for ANNEX_B compatibility.

Severity Info

Explanation When configuring Service Module cards, users should be aware that certain attributes are not compatible with certain cards. When trying the change these attributes through commands at the CLI, the command is rejected. During upgrade or when an AutoProv profile is set so incompatible attributes will be applied, the system will change the attribute to ensure compatibility, and a log is produced. In this message, Echo Cancellation (EC) was changed to OFF for an ANNEX_B card.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.37.2 Not Applicable

Message MODE changed from ADSL2+ to GDMT for ANNEX_B compatibility.

Severity Info

Explanation For a general description, refer to the Message starting with 'EC changed.' In this example, the mode was changed by the system to GDMT.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.38 PSPN003 - atnPSpanDefectRaised

2.38.1 ARP Resolution Failed

Message ARP Resolution Failed

Severity Minor

Explanation The PSPAN was not able to resolve the MAC address of the peer (or the gateway) using the ARP protocol. This may indicate that the peer (or the gateway) is down, or that the intervening network is down.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	PSPAN	Failed	Minor

2.38.2 DNS resolution failed

Message Not Applicable

Severity Minor

Explanation The IP protocol software on the card was not able to resolve the domain name of the peer (or the gateway) using the DNS protocol. This may indicate a problem with the DNS server, the domain name may be invalid, or there may be a problem with the intervening network.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	PSPAN	Failed	Minor

2.38.3 DNS Server Timed Out

Message To Be Supplied

Severity Minor

Explanation Not supported in R5.0. [STILL TRUE?][To Be Supplied]

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	PSPAN	Failed	Minor

2.38.4 PSPAN Configuration Failed

Message To Be Supplied

Severity Minor

Explanation The system failed to configure the hardware with provisioned PSPAN data. This will impact service provided by the PSPAN.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	PSPAN	Failed	Minor

2.38.5 PSPAN does not have a connection

Message To Be Supplied

Severity Minor

Explanation The PSPAN is not connected to a DS1/E1 port. A connection is required for the PSPAN to generate or receive packets from the network.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	PSPAN	Failed	Minor

2.38.6 PSPAN Egress Path Failed

Message To Be Supplied

Severity Minor

Explanation This indicates that the PSPAN has not received any packets from the peer since it was enabled / connected. This might indicate that the peer is not yet configured, or is misconfigured.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	PSPAN	Failed	Minor

2.38.7 PSPAN Ingress Path Failed

Message To Be Supplied

Severity Minor

Explanation This indicates that the PSPAN has not been able to send any packets into the network. This is a service impacting condition, and is most likely due to internal hardware failures.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	PSPAN	Failed	Minor

2.38.8 PSPAN LOPS

Message To Be Supplied

Severity Minor

Explanation This indicates a local "Loss of Packet Stream" fault on the PSPAN. This means that the PSPAN detected 10 or more missing packets per second for 3 consecutive seconds. This fault will be cleared when the PSPAN detects no missing packets for 10 consecutive seconds. The presence of this fault indicates service is impacted.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	PSPAN	Failed	Major

2.38.9 PSPAN Remote LOPS

Message To Be Supplied

Severity Minor

Explanation This indicates that the peer CES8 card is reporting Loss Of Packet Stream (LOPS). This means that properly formatted packets generated by this CES8 card are not reaching the peer CES8 card. This may be a result of changed in network conditions or configuration.

Action Perform the following:

1. Verify that you can PING the peer CES8 card's IP address from the local CES8 card's IP address.
2. If changes have been made to the PSPAN configuration, verify that the settings are consistent on the local and the peer.

Alarms The following components are affected:

	Component	Status	Alarm
•	PSPAN	Failed	Major

2.38.10 PSPAN Timing Reference Degraded

Message To Be Supplied

Severity Minor

Explanation The PSPAN's provisioned timing reference cannot provide a reliable timing reference. The interface is being timed from an alternate reference that is not known to be locked to the provisioned source.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	PSPAN	Degraded	Minor

2.38.11 PSPAN Timing Reference failed

Message To Be Supplied

Severity Minor

Explanation Not supported in R5.0. [STILL TRUE?][To Be Supplied]

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	PSPAN	Failed	Minor

2.39 SHLF001 - atnShelfFaultRaised

2.39.1 Can Not Read Temperature Sensors

Message Shelf Failure Raised\nReason \ Code: %1$s

Severity Major

Explanation The system cannot read its internal temperature.

Action Perform the following:

1. Search for a FAN log (e.g., ** FAN001 2003-11-14 17:06:37 8172 FAULT Description: Fan Module Failure Raised Reason Code: Fan Module Not Present).
2. Replace the CFC card.
3. Refer to Section 5. [STILL TRUE?][To Be Supplied]

Alarms The following components are affected:

	Component	Status	Alarm
•	Shelf	N/A	Major

2.39.2 High Shelf Temperature

Message To Be Supplied

Severity Critical

Explanation The ambient temperature has exceeded the acceptable temperature range.

Action Perform the following:

1. Reduce ambient temperature.
2. Check the fans.

Alarms The following components are affected:

	Component	Status	Alarm
•	Shelf	N/A	Major

2.39.3 High Temperature

Message To Be Supplied

Severity Major

Explanation To Be Supplied.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

	Component	Status	Alarm
•	Shelf	N/A	Major

2.40 SHLF008 - atnDryContactRaised

2.40.1 Unknown

Message Dry Contact: n: OPEN

Severity Major

Explanation The Dry Contact fault has been raised for an open contact condition. The reason code and severity will depend on the user provisioning for the specific dry contact condition.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.41 SHLF009 - atnDryContactCleared

2.41.1 Unknown

Message Unknown

Severity Info

Explanation The Dry Contact fault has cleared. The reason code will depend on the original fault.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.41.2 Unknown

Message Dry Contact: n: CLOSED

Severity Clear

Explanation The Dry Contact fault has been raised for a closed contact condition. The reason code and severity will depend on the user provisioning for the specific dry contact condition.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.42 SYS004 - atnMediaLogStreamError

2.42.1 CFlash Failed

Message Compact Flash Failed

Severity Major

Explanation To Be Supplied.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

	Component	Status	Alarm
•	CFC24	Degraded	Minor
•	CFC24	Degraded	Minor

2.43 SYS009 - atnShelfFaultRaised

2.43.1 Packet Overflow

Message System: Raised %1$s

Severity Critical

Explanation An extremely high volume of traffic is being received by the system, exceeding the processing and packet switching capacity of the system, resulting in packet loss.

Action Perform the following:

1. Reduce traffic on the system

Alarms The following components are affected:

	Component	Status	Alarm
•	None		

2.44 XDSL001 - HDSL2SHDSLPERFLOSWSTHRESH

2.44.1 Not Applicable

Message STU-C Loss of Sync Word Seconds (LOSWS) TCA

Severity Info

Explanation The threshold set for the statistic has been exceeded over the current 15 minute interval.

Action Perform the following:

1. Check to ensure the threshold has been set to the appropriate level.
2. If the threshold is appropriate, check the line facilities.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.45 XDSL002 - HDSL2SHDSLPERFCRCANOMALIESTHRESH

2.45.1 Not Applicable

Message STU-C CRC Anomalies TCA

Severity Info

Explanation The threshold set for the statistic has been exceeded over the current 15 minute interval.

Action Perform the following:

1. Check to ensure the threshold has been set to the appropriate level.
2. If the threshold is appropriate, check the line facilities.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.46 XDSL003 - HDSL2SHDSLPERFESTHRESH

2.46.1 Not Applicable

Message STU-C Errored Seconds (ES) TCA

Severity Info

Explanation The threshold set for the statistic has been exceeded over the current 15 minute interval.

Action Perform the following:

1. Check to ensure the threshold has been set to the appropriate level.
2. If the threshold is appropriate, check the line facilities.

Alarms The following components are affected:

Component Status Alarm

- None

2.47 XDSL004 - HDSL2SHDSLPERFSESTHRESH

2.47.1 Not Applicable

Message STU-C Severely Errored Seconds (SES) TCA

Severity Info

Explanation The threshold set for the statistic has been exceeded over the current 15 minute interval.

Action Perform the following:

1. Check to ensure the threshold has been set to the appropriate level.
2. If the threshold is appropriate, check the line facilities.

Alarms The following components are affected:

Component Status Alarm

- None

2.48 XDSL005 - HDSL2SHDSLPERFUASTHRESH

2.48.1 Not Applicable

Message STU-C Unavailable Seconds (UAS) TCA

Severity Info

Explanation The threshold set for the statistic has been exceeded over the current 15 minute interval.

Action Perform the following:

1. Check to ensure the threshold has been set to the appropriate level.
2. If the threshold is appropriate, check the line facilities.

Alarms The following components are affected:

Component Status Alarm

- None

2.49 XDSL006 - HDSL2SHDSLPERFLOSWSTHRESH

2.49.1 Not Applicable

Message STU-R Loss of Sync Word Seconds (LOSWS) TCA

Severity Info

Explanation The threshold set for the statistic has been exceeded over the current 15 minute interval.

Action Perform the following:

1. Check to ensure the threshold has been set to the appropriate level.
2. If the threshold is appropriate, check the line facilities.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.50 XDSL007 - HDSL2SHDSLPERFCRCANOMALIESTHRESH

2.50.1 Not Applicable

Message STU-R CRC Anomalies TCA

Severity Info

Explanation To Be Supplied.

Action Perform the following:

1. To Be Supplied

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.50.2 Not Applicable

Message STU-R CRC Anomalies TCA

Severity Info

Explanation The threshold set for the statistic has been exceeded over the current 15 minute interval.

Action Perform the following:

1. Check to ensure the threshold has been set to the appropriate level.

2. If the threshold is appropriate, check the line facilities.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.51 XDSL008 - HDSL2SHDSLPERFESTHRESH

2.51.1 Not Applicable

Message STU-R Errored Seconds (ES) TCA

Severity Info

Explanation The threshold set for the statistic has been exceeded over the current 15 minute interval.

Action Perform the following:

1. Check to ensure the threshold has been set to the appropriate level.
2. If the threshold is appropriate, check the line facilities.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.52 XDSL009 - HDSL2SHDSLPERFSESTHRESH

2.52.1 Not Applicable

Message STU-R Severely Errored Seconds (SES) TCA

Severity Info

Explanation The threshold set for the statistic has been exceeded over the current 15 minute interval.

Action Perform the following:

1. Check to ensure the threshold has been set to the appropriate level.
2. If the threshold is appropriate, check the line facilities.

Alarms The following components are affected:

Component	Status	Alarm
• None		

2.53 XDSL010 - HDSL2SHDSLPERFUASTHRESH

2.53.1 Not Applicable

Message STU-R Unavailable Seconds (UAS) TCA

Severity Info

Explanation The threshold set for the statistic has been exceeded over the current 15 minute interval.

Action Perform the following:

1. Check to ensure the threshold has been set to the appropriate level.
2. If the threshold is appropriate, check the line facilities.

Alarms The following components are affected:

	Component	Status	Alarm
•	None		

2.54 XDSL018 - xdslPortQualityRetrain

2.54.1 Retrain: Line Quality

Message Port Information

Severity Info

Explanation The Errored Seconds is too high, so the xDSL port is disabled and enabled to retrain the link. The xDSL Quality Audit will try to retrain the port to an acceptable level.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

	Component	Status	Alarm
•	ADSL Port	Online	None
•	SHDSL Port	Online	None
•	VDSL Port	Online	None

2.55 XDSL019 - xdslPortStuckHandShakeRetrain

2.55.1 Retrain: Handshake Stuck

Message Port Information

Severity Info

Explanation The physical layer connection failed, so the xDSL port is disabled and enabled to retrain the link.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

Component	Status	Alarm
• ADSL Port	Online	None
• SHDSL Port	Online	None
• VDSL Port	Online	None

2.56 XDSL020 - xdslPortMinDownRateRetrain

2.56.1 Retrain: Minimum Downstream Rate

Message Port Information

Severity Info

Explanation The connect rate is below the provisioned minimum downstream rate, so the xDSL port will be disabled and enabled to retrain the link.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

Component	Status	Alarm
• ADSL Port	Online	None
• SHDSL Port	Online	None
• VDSL Port	Online	None

2.57 XDSL021 - xdsllossofmarginretrain

2.57.1 Retrain: SNR Margin Threshold

Message Port Information

Severity Info

Explanation For the VDSL24 port, this alarm appears when the SNR margin drops below the set minimum SNR margin.

Action Perform the following:

1. No action is required.

Alarms The following components are affected:

Component	Status	Alarm
• None		

5. NMS Logs

1 Overview

The AlliedView NMS allows network administrators to query and control both Allied Telesis and non-Allied Telesis devices in their network. Moreover, there are two types of NSM products available;

- Service Provider - This includes all NMS features
- Enterprise Edition - The Enterprise Edition is introduced primarily for the smaller enterprise customer managing a network of less than 100 devices. All features of the Service Provider Edition (SE) are supported in the Enterprise Edition with the exception of customer provisioning of voice, video, and data services.

Note: Refer to the AlliedView NMS Administration Guide for complete information.

Since all NMS logs have the same category (NMS) and the concept of trap is not applicable, the logs are listed as follows:

Type of NMS activity - This can be divided into these areas:

- Status Polling of Devices
- Discovery of Devices
- NMS Backup
- Device Backup

For each area, abbreviated log messages are listed, and each includes:

- Complete Log Message
- Severity
- Explanation

2 Device Backup

2.1 Device Backup Failed

Message	Device Backup Failed! -error detail-
Severity	Major
Explanation	See error detail for steps to take. Manually clear this alarm after doing a successful backup.

3 Discovery

3.1 SNMP Error Code

Message	(SNMP error code): Error fetching device information Some of the properties may be incorrect.
Severity	Major
Explanation	Verify SNMP to device and Rediscover Device.

3.2 Unable to Detect MO

Message	Unable to update MO (status = false)
Severity	Major
Explanation	If problem persists call Allied Telesis NMS support.

3.3 Max. Allowed Node Limit Reached

Message	Max. Allowed Node Limit of 4 Reached. Please Contact Allied Telesyn Networks to Upgrade your node limit.
Severity	Major
Explanation	To be Supplied - SE versus EE on Network objects, Allied Telesis Nodes discovered using ICMP, and non-Allied Telesis devices are not counted against this limit. To change this limit requires an update to the NMS license, and should be done with help from Allied Telesis.

3.4 Unable to login to device

Message	Unable to login to device. Add an NMS recognized userid/password to the device OR configure the NMS to recognize an account of the device
Severity	Warning
Explanation	Add an NMS recognized userid/password to the device or configure the NMS to recognize an account of the device.

3.5 Detected DUPLICATE IP

Message	Detected DUPLICATE IP. (IP addr) in node (device name) is a duplicate of (device name)
Severity	Warning
Explanation	If this is an unintentional duplicate then change the IP on one of the devices and rediscover both devices

4 NMS backup

4.1 Cannot locate directory

Message NMS Backup Failure -- Can't locate conf/AT_NmsBackupFiles.conf (no files backed up)

Severity Major

Explanation If problem persists call Allied Telesis NMS support.

4.2 Cannot create directory

Message NMS Backup Failure -- Unable to create directory path needed for BACKUP_DESTINATION: -path-

Severity Warning

Explanation Verify that NMS process has write permissions for the directory.

4.3 IO Exception to access NMS Home directory

Message NMS Backup Failure -- IO Exception occurred while attempting to access: -NMS Home directory-

Severity Warning

Explanation Verify that the NMS process has read permissions for the directory where it is installed.

4.4 IO Exception to access backup directory

Message NMS Backup Failure -- IO Exception occurred reading: conf/AT_NmsBackupFiles.conf (no files backed up)

Severity Warning

Explanation If problem persists call Allied Telesis NMS support.

4.5 Cannot locate directory

Message NMS Backup Failure -- NmsBackup can not locate directory: specified in AT_NmsBackupFiles.conf (directory skipped)

Severity Warning

Explanation Verify that source directory exists

4.6 Security Exception

Message NMS Backup Failure -- A Security Exception has occurred opening: conf/AT_NmsBackupFiles.conf (no files backed up)

Severity Major

Explanation If problem persists call Allied Telesis NMS support.

4.7 Cannot complete backup

Message NMS Backup Failure -- Database backup could not be completed (Check DB table sizes and see log for details)

Severity Warning

Explanation Check the database table sizes and see logs for details

4.8 Cannot create directory for directory copy

Message NMS Backup Failure -- Unable to create directory path needed for directory copy (from -source- to -destination-)

Severity Warning

Explanation If problem persists call Allied Telesis NMS support.

5 Status Poll

5.1 At least one Node in failure state

Message At least one node in this network is in failure state

Severity Major

Explanation Check the Alarm view to see which device is affected. Then go to the Physical View and perform a View Chassis as well as a right click to select Alarms and Events. Go to the System Log Events view and sort by Source. Look at the associated logs and refer again to this Log Manual.

5.2 Interface Failure

Message Interface Failure. Status Poll Failed

Severity Major

Explanation Check the Failure Object in the Alarm view to see which device is affected. Then go to the Physical View and perform a View Chassis, since this may mean a port is down. Right click on the device and select Alarms and Events. Go to the System Log Events view and sort by Source. Look at the associated logs and refer again to this Log Manual.

5.3 Node Failure

Message Node Failure. This probably means one or more interfaces have failed.

Severity	Major
Explanation	Check the Failure Object in the Alarm view to see which device is affected. Then go to the Physical View and perform a View Chassis as well as a right click to select Alarms and Events. Go to the System Log Events view and sort by Source. Look at the associated logs and refer again to this Log Manual.

6 Other

6.1 Upload Config Failed

Message	Upload Config Failed! -error detail-
Severity	Major
Explanation	See error detail for steps to take. Manually clear this alarm after doing a successful backup.